KOMMISJONENS GJENNOMFØRINGSBESLUTNING (EU) 2016/1250 **2019/EØS/62/50**

av 12. juli 2016

i henhold til europaparlaments- og rådsdirektiv 95/46/EF om tilstrekkeligheten av det vernet som sikres ved Privacy Shield-avtalen mellom EU og De forente stater

[meddelt under nummer K(2016) 4176](*)

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger([1]), særlig artikkel 25 nr. 6,

etter samråd med EUs datatilsyn([2]) og ut fra følgende betraktninger:

1. INNLEDNING

1) Ved direktiv 95/46/EF fastsettes det regler for overføring av personopplysninger fra medlemsstater til tredjestater i den grad slike overføringer omfattes av direktivets virkeområde.

2) Formålet med artikkel 1 i direktiv 95/46/EF samt betraktning 2 og 10 i direktivets preambel er ikke bare å sikre et effektivt og fullstendig vern av fysiske personers grunnleggende rettigheter og friheter, særlig den grunnleggende retten til respekt for privatliv i forbindelse med behandling av personopplysninger, men også et høyt nivå for vern av nevnte grunnleggende rettigheter og friheter([3]).

3) Viktigheten av både den grunnleggende retten til respekt for privatliv som sikres ved artikkel 7, og den grunnleggende retten til vern av personopplysninger som sikres ved artikkel 8 i Den europeiske unions pakt om grunnleggende rettigheter, er blitt understreket i Domstolens rettspraksis([4]).

4) I henhold til artikkel 25 nr. 1 i direktiv 95/46/EF skal medlemsstatene fastsette bestemmelser om at overføring av personopplysninger til en tredjestat kan finne sted bare dersom den berørte tredjestaten sikrer et tilstrekkelig beskyttelsesnivå, og dersom medlemsstatens nasjonale rett som gjennomfører andre bestemmelser i direktivet, er overholdt før overføringen. Kommisjonen kan fastslå at en tredjestat sikrer et slikt tilstrekkelig beskyttelsesnivå på grunnlag av tredjestatens nasjonale rett eller de internasjonale forpliktelsene den har inngått med henblikk på vern av privatpersoners rettigheter. Dersom dette er tilfellet, og uten at det berører overholdelsen av de nasjonale bestemmelsene vedtatt i henhold til andre bestemmelser i direktivet, kan personopplysninger overføres fra medlemsstatene uten at det må stilles ytterligere garantier.

(*) Denne unionsrettsakten, kunngjort i EUT L 207 av 1.8.2016, s. 1, er omhandlet i EØS-komiteens beslutning nr. 144/2017 av 7. juli 2017 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester), se EØS-tillegget til *Den europeiske unions tidende* nr. 40 av 16.5.2019, s. 45.

([1]) EFT L 281 av 23.11.1995, s. 31.

([2]) Se uttalelse 4/2016 om Privacy Shield-avtalen mellom EU og De forente stater – utkast til beslutning om tilstrekkelig beskyttelsesnivå, offentliggjort 30. mai 2016.

([3]) Sak C-362/14, Maximillian Schrems v Data Protection Commissioner («Schrems»), EU:C:2015:650, nr. 39.

([4]) Sak C-553/07, Rijkeboer, EU:C:2009:293, nr. 47; forente saker C-293/12 og C-594/12, Digital Rights Ireland and Others, EU:C:2014:238, nr. 53; Sak C-131/12, Google Spain and Google, EU:C:2014:317, nr. 53, 66 og 74.

5) I henhold til artikkel 25 nr. 2 i direktiv 95/46/EF skal vurderingen av om nivået for vern av personopplysninger i en tredjestat er tilstrekkelig, foretas på bakgrunn av alle forhold som har innflytelse på en overføring eller på en kategori overføringer, herunder gjeldende rettsregler, både alminnelige regler og sektorregler, som gjelder i den aktuelle tredjestaten.

6) I kommisjonsvedtak 2000/520/EF([5]) ble det med hensyn til artikkel 25 nr. 2 i direktiv 95/46/EF ansett at «trygg havn»-prinsippene for personvern gjennomført i samsvar med veiledningen som gis i de såkalte «vanlige spørsmålene» utstedt av det amerikanske handelsdepartementet, gir et tilstrekkelig nivå for vern av personopplysninger som overføres fra Unionen til organisasjoner som er etablert i De forente stater.

7) I sine meldinger KOM(2013) 846 endelig utgave([6]) og KOM(2013) 847 endelig utgave av 27. november 2013([7]) anså Kommisjonen at grunnlaget for «trygg havn»-ordningen måtte gjennomgås på nytt og styrkes på bakgrunn av en rekke faktorer, herunder den kraftige økningen i datastrømmene og den avgjørende betydningen disse har for den transatlantiske økonomien, den raske veksten i antall amerikanske selskaper som har sluttet seg til «trygg havn»-ordningen, og ny informasjon om omfanget og utbredelsen av visse amerikanske etterretningsprogrammer som har ført til at det er reist spørsmål ved beskyttelsesnivået som sikres ved ordningen. Kommisjonen har i tillegg fastslått at «trygg havn»-ordningen har en rekke mangler.

8) På grunnlag av dokumentasjon som Kommisjonen har innhentet, herunder informasjon fra arbeidet til EUs og De forente staters kontaktgruppe for personvern([8]) og informasjon om amerikanske etterretningsprogrammer framlagt for EUs og De forente staters ad hoc-arbeidsgruppe([9]), har Kommisjonen utarbeidet 13 anbefalinger med henblikk på en ny gjennomgåelse av «trygg havn»-ordningen. I disse anbefalingene er det fokusert på å styrke de vesentlige personvernprinsippene, gjøre personvernprogrammene til amerikanske egensertifiserte selskaper mer gjennomsiktige, bedre amerikanske myndigheters tilsyn med samt overvåking av at nevnte prinsipper overholdes og håndheving av dette, innføring av økonomisk overkommelige tvisteløsningsmekanismer og behovet for å sikre at unntaket som gjelder nasjonal sikkerhet fastsatt i vedtak 2000/520/EF, bare anvendes når det er strengt nødvendig og forholdsmessig.

9) I sin dom av 6. oktober 2015 i sak C-362/14, *Maximillian Schrems* v *Data Protection Commissioner*([10]), erklærte Den europeiske unions domstol vedtak 2000/520/EF ugyldig. Uten å undersøke innholdet i «trygg havn»-prinsippene for personvern anså Domstolen at Kommisjonen i nevnte vedtak ikke hadde angitt at De forente stater faktisk «sikret» et tilstrekkelig beskyttelsesnivå gjennom sin nasjonale rett eller de internasjonale forpliktelsene som De forente stater har inngått([11]).

10) I denne forbindelse forklarte Domstolen at det med termen «tilstrekkelig vernenivå» i artikkel 25 nr. 6 i direktiv 95/46/EF ikke menes et beskyttelsesnivå som er identisk med det som sikres i EUs rettsorden, men at den må forstås som at det kreves at tredjestaten sikrer et nivå for vern av grunnleggende rettigheter og friheter som «i hovedtrekk tilsvarer» det som sikres i Unionen i henhold til direktiv 95/46/EF, sammenholdt med pakten om grunnleggende rettigheter. Selv om midlene som nevnte tredjestat anvender i denne forbindelse, kan avvike fra dem som anvendes i Unionen, må nevnte midler imidlertid være effektive i praksis([12]).

11) Domstolen kritiserte mangelen på tilstrekkelige konklusjoner i vedtak 2000/520/EF med hensyn til om det i De forente stater finnes statlige regler beregnet på å begrense eventuelle inngrep i de grunnleggende rettighetene til personer som får sine opplysninger overført fra Unionen til De forente stater, hvilke inngrep landets offentlige organer har rett til å foreta når de forfølger berettigede mål, f.eks. nasjonal sikkerhet, og om det foreligger et effektivt rettslig vern mot inngrep av denne art([13]).

([5]) Kommisjonsvedtak 2000/520/EF av 26. juli 2000 i henhold til europaparlaments- og rådsdirektiv 95/46/EF om tilstrekkeligheten av den beskyttelse som oppnås ved «trygg havn»-prinsippene for personvern og tilhørende vanlige spørsmål fra De forente staters handelsdepartement (EFT L 215 av 28.8.2000, s. 7).

([6]) Melding fra Kommisjonen til Europaparlamentet og Rådet om gjenoppbygging av tilliten til datastrømmene mellom EU og USA, KOM(2013) 846 endelig utgave av 27. november 2013.

([7]) Melding fra Kommisjonen til Europaparlamentet og Rådet om hvordan «trygg havn»-ordningen fungerer med hensyn til EU-borgere og selskaper som er etablert i EU, KOM(2013) 847 endelig utgave av 27. november 2013.

([8]) Se f.eks. Rådet for Den europeiske union, sluttrapport fra EU og De forente staters høynivåkontaktgruppe for informasjonsutveksling og personvern og vern av personopplysninger, note 9831/08, 28. mai 2008, tilgjengelig på ttp://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Rapport om konklusjonene fra EU-formennene for EU og De forente staters ad hoc-arbeidsgruppe om personvern, 27. november 2013, tilgjengelig på http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Se fotnote 3.

([11]) Schrems, nr. 97.

([12]) Schrems, nr. 73–74.

([13]) Schrems, nr. 88–89.

12) I 2014 innledet Kommisjonen forhandlinger med amerikanske myndigheter for å drøfte en styrking av «trygg havn»-ordningen i samsvar med de 13 anbefalingene i melding KOM(2013) 847 endelig utgave. Etter dommen i *Schrems*-saken i Den europeiske unions domstol ble disse forhandlingene styrket med henblikk på en mulig ny beslutning om tilstrekkelig beskyttelsesnivå som vil oppfylle kravene i artikkel 25 i direktiv 95/46/EF slik Domstolen har tolket dem. Dokumentene som er vedlagt denne beslutning, og som også vil bli offentliggjort i De forente staters *Federal Register*, er resultatet av disse drøftingene. Personvernprinsippene (vedlegg II) og de offisielle redegjørelsene og forpliktende tilsagnene fra forskjellige amerikanske myndigheter i dokumentene i vedlegg I og III–VII utgjør «Privacy Shield-avtalen mellom EU og De forente stater».

13) Kommisjonen har foretatt en grundig analyse av amerikansk rett og praksis, herunder nevnte offisielle redegjørelser og forpliktende tilsagn. På grunnlag av det som framgår av betraktning 136–140, konkluderer Kommisjonen med at De forente stater sikrer et tilstrekkelig nivå for vern av personopplysninger som overføres fra Unionen til egensertifiserte organisasjoner i De forente stater innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater.

2. **PRIVACY SHIELD-AVTALEN MELLOM EU OG DE FORENTE STATER**

14) Privacy Shield-avtalen mellom EU og De forente stater bygger på et egensertifiseringssystem der amerikanske organisasjoner forplikter seg til å følge en rekke personvernprinsipper – prinsipper i rammeverket for Privacy Shield-avtalen mellom EU og De forente stater, herunder supplerende prinsipper (heretter samlet kalt «prinsippene») – utstedt av det amerikanske handelsdepartementet og angitt i vedlegg II til denne beslutning. Avtalen får anvendelse på både behandlingsansvarlige og databehandlere (representanter) og er underlagt det særlige vilkåret at databehandlere må være avtalebundet til bare å handle på instruks fra den behandlingsansvarlige i EU og bistå sistnevnte med å besvare anmodninger fra privatpersoner som utøver sine rettigheter i henhold til prinsippene([14]).

15) Uten at det berører plikten til å overholde de nasjonale bestemmelsene vedtatt i henhold til direktiv 95/46/EF, medfører denne beslutning at overføringer fra en behandlingsansvarlig eller en databehandler i Unionen til organisasjoner i De forente stater som ved egensertifisering ved det amerikanske handelsdepartementet har sluttet seg til prinsippene og forpliktet seg til å overholde dem, er tillatt. Prinsippene gjelder bare behandling av personopplysninger som utføres av amerikanske organisasjoner i den grad slike organisasjoners behandling ikke omfattes av Unionens regelverk([15]). Privacy Shield-avtalen påvirker ikke anvendelsen av Unionens regelverk for behandling av personopplysninger i medlemsstatene([16]).

([14]) Se vedlegg II avsnitt III nr. 10 bokstav a). I tråd med definisjonen i avsnitt I nr. 8 bokstav c) skal den behandlingsansvarlige i EU bestemme formålet med og midlene for behandling av personopplysningene. Videre skal det i avtalen med representanten tydelig angis om videreoverføring er tillatt (se avsnitt III nr. 10 bokstav a) ii) nr. 2.).

([15]) Dette får også anvendelse på overføring fra Unionen av opplysninger om menneskelige ressurser i forbindelse med et arbeidsforhold. Selv om det i prinsippene understrekes at arbeidsgiveren i EU har «hovedansvaret» (se vedlegg II avsnitt III nr. 9 bokstav d) i)), presiseres det også at vedkommendes må opptre i henhold til gjeldende regler i Unionen og/eller den berørte medlemsstaten, ikke prinsippene. Se vedlegg II avsnitt III nr. 9 bokstav a) i), b) ii), c) i), d) i).

([16]) Dette får også anvendelse på behandling som skjer ved hjelp av utstyr som befinner seg i Unionen, men som brukes av en organisasjon som er etablert utenfor Unionen (se artikkel 4 nr. 1 bokstav c) i direktiv 95/46/EF). Fra og med 25. mai 2018 får den generelle personvernforordningen (GDPR) anvendelse på behandling av personopplysninger i) som foretas i forbindelse med virksomheten til en behandlingsansvarlig eller en databehandler i Unionen (selv om behandlingen finner sted i De forente stater), eller ii) om registrerte som befinner seg i Unionen, og som foretas av en behandlingsansvarlig eller en databehandler som ikke er etablert i Unionen, dersom behandlingsaktivitetene er knyttet til a) tilbud av varer eller tjenester, uavhengig av om det kreves betaling fra den registrerte eller ikke, eller b) monitorering av deres atferd i den grad deres atferd finner sted i Unionen. Se artikkel 3 nr. 1 og 2 i europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

16) Det vern av personopplysninger som Privacy Shield-avtalen gir, gjelder alle registrerte i EU([17]) som har fått sine personopplysninger overført fra Unionen til organisasjoner i De forente stater som ved egensertifisering ved det amerikanske handelsdepartementet har sluttet seg til prinsippene.

17) Prinsippene får anvendelse umiddelbart etter sertifisering. Det eneste unntaket gjelder prinsippet om ansvar for videreoverføring dersom en organisasjon som ved egensertifisering har sluttet seg til Privacy Shield-ordningen, allerede har handelsforbindelser med tredjeparter. Det kan ta litt tid å bringe nevnte handelsforbindelser i samsvar med reglene som får anvendelse i henhold til prinsippet om ansvar for videreoverføring, men organisasjonen plikter å gjøre dette så snart som mulig og under alle omstendigheter senest ni måneder etter egensertifisering (forutsatt at dette skjer i løpet av de to første månedene etter at Privacy Shield-avtalen har trådt i kraft). I denne overgangsperioden må organisasjonen anvende prinsippet om opplysningsplikt og valgmulighet (og på den måten gi den registrerte i EU mulighet til å motsette seg behandling) og, når personopplysninger overføres til en tredjepart som fungerer som representant, sørge for at sistnevnte minst sikrer det samme beskyttelsesnivået som det som kreves i prinsippene([18]). Denne overgangsperioden sikrer en rimelig og hensiktsmessig balanse mellom respekten for den grunnleggende retten til vern av personopplysninger og virksomheters berettigede behov for tilstrekkelig tid til å tilpasse seg den nye ordningen når dette også avhenger av deres handelsforbindelser med tredjeparter.

18) Systemet vil bli forvaltet og overvåket av det amerikanske handelsdepartementet på grunnlag av dets forpliktelser angitt i redegjørelsene fra den amerikanske handelsministeren (vedlegg I til denne beslutning). Når det gjelder håndheving av prinsippene, har Federal Trade Commission (FTC) og det amerikanske transportdepartementet avgitt redegjørelser som er angitt i vedlegg IV og V til denne beslutning.

2.1. *Personvernprinsipper*

19) Som et ledd i egensertifiseringen som skal utføres i henhold til Privacy Shield-avtalen mellom EU og De forente stater, skal organisasjoner forplikte seg til å overholde prinsippene([19]).

20) I henhold til *prinsippet om opplysningsplikt* plikter organisasjoner å informere registrerte om en rekke sentrale elementer knyttet til behandlingen av deres personopplysninger (f.eks. hvilken type opplysninger som samles inn, formålet med behandlingen, retten til innsyn og valgmulighet, vilkår for videreoverføring og ansvar). Ytterligere garantier får anvendelse, særlig kravet om at organisasjoner skal offentliggjøre sine personvernprogrammer (som skal gjenspeile prinsippene) og angi lenker til nettstedet til det amerikanske handelsdepartementet (med ytterligere opplysninger om egensertifisering, registrertes rettigheter og tilgjengelige klagemekanismer), Privacy Shield-listen (omhandlet i betraktning 30) og nettstedet til et egnet alternativt tvisteløsningsorgan.

21) I henhold til *prinsippet om dataintegritet og formålsbegrensning* skal personopplysninger begrenses til det som er relevant for formålet med behandlingen, samt være pålitelige med henblikk på den planlagte bruken samt riktige, fullstendige og oppdaterte. En organisasjon kan ikke behandle personopplysninger på en måte som er uforenlig med formålet som opplysningene opprinnelig ble samlet inn for, eller et formål som den registrerte senere har godkjent. Organisasjoner skal sikre at personopplysningene er pålitelige med henblikk på den planlagte bruken samt at de er korrekte, fullstendige og oppdaterte.

([17]) Denne beslutning er relevant for EØS. Avtalen om Det europeiske økonomiske samarbeidsområde (EØS-avtalen) utvider Den europeiske unions indre marked til også å omfatte de tre EØS-statene Island, Liechtenstein og Norge. Unionens personvernregelverk, herunder direktiv 95/46/EF, inngår i EØS-avtalen og er innlemmet i vedlegg XI til avtalen. EØS-komiteen skal beslutte om denne beslutning skal innlemmes i EØS-avtalen. Så snart denne beslutning får anvendelse på Island, Liechtenstein og Norge, vil Privacy Shield-avtalen mellom EU og De forente stater også omfatte disse tre statene, og henvisninger til EU og EUs medlemsstater i Privacy Shield-pakken skal leses som at dette også omfatter Island, Liechtenstein og Norge.

([18]) Se vedlegg II avsnitt III nr. 6 bokstav e).

([19]) Særlige regler som gir ytterligere garantier, får anvendelse på opplysninger om menneskelige ressurser som samles inn i forbindelse med et arbeidsforhold, som fastsatt i det supplerende prinsippet om «opplysninger om menneskelige ressurser» i personvernprinsippene (se vedlegg II avsnitt III nr. 9). Arbeidsgivere bør f.eks. ta hensyn til de ansattes ønsker når det gjelder vern av personopplysninger, ved å begrense tilgangen til personopplysningene, anonymisere visse opplysninger eller bruke koder eller pseudonymer. Men enda viktigere er det at organisasjoner skal samarbeide med og følge anbefalingene fra Unionens personvernmyndigheter når det gjelder slike opplysninger.

22) Dersom et nytt (endret) formål er vesentlig forskjellig fra, men fremdeles er forenlig med det opprinnelige formålet, gir *prinsippet om valgmulighet* de registrerte rett til å reservere seg. *Prinsippet om valgmulighet* erstatter ikke det uttrykkelige forbudet mot uforenlig behandling([20]). Med hensyn til direkte markedsføring gjelder det særlig regler som på generelt grunnlag gjør det mulig «når som helst» å reservere seg mot at personopplysninger brukes til dette([21]). Når det gjelder sensitive opplysninger, skal organisasjoner normalt innhente den registrertes uttrykkelige samtykke.

23) I henhold til *prinsippet om dataintegritet og formålsbegrensning* kan personopplysninger oppbevares i en form som identifiserer en person eller gjør vedkommende identifiserbar (dvs. i form av personopplysninger), bare så lenge det tjener formålet/formålene som opplysningene opprinnelig ble samlet inn for, eller formål som senere er blitt godkjent. Denne plikten hindrer ikke Privacy Shield-organisasjoner i å fortsette å behandle personopplysninger i lengre perioder, men bare så lenge og i det omfang nevnte behandling med rimelighet tjener et av følgende særlige formål: arkivformål i allmennhetens interesse, journalistikk, litteratur og kunst, vitenskapelig og historisk forskning samt statistisk analyse. En mer langvarig lagring av personopplysninger med sikte på et av disse formålene omfattes av garantiene fastsatt i prinsippene.

24) I henhold til *prinsippet om sikkerhet* skal organisasjoner som oppretter, forvalter, bruker eller sprer personopplysninger, treffe «rimelige og hensiktsmessige» sikkerhetstiltak der det tas hensyn til risikoene forbundet med behandlingen samt opplysningenes art. Dersom behandlingen settes ut til en underleverandør, skal organisasjonene inngå en avtale med underleverandøren som garanterer det samme beskyttelsesnivået som det som er fastsatt i prinsippene, og treffe tiltak for å sikre at behandlingen gjennomføres på riktig måte.

25) I henhold til *prinsippet om innsyn*([22]) har registrerte, uten at det er nødvendig å begrunne dette og mot et rimelig gebyr, rett til å få opplyst fra en organisasjon om den behandler personopplysninger om dem, og til å få utlevert opplysningene innen rimelig tid. Denne retten kan bare begrenses i særlige tilfeller; enhver nekting eller begrensning av retten til innsyn skal være nødvendig og behørig begrunnet, og det er organisasjonen som skal bære byrden for å dokumentere at disse kravene er oppfylt. Registrerte skal ha mulighet til å få rettet, endret eller slettet uriktige personopplysninger eller personopplysninger som er blitt behandlet i strid med prinsippene. På områder der det er stor sannsynlighet for at selskaper bruker automatisert behandling av personopplysninger for å treffe avgjørelser som påvirker privatpersoner (f.eks. om innvilgelse av kreditt, tilbud om boliglån, ansettelse), sikrer amerikansk rett et særlig vern mot negative avgjørelser([23]). Generelt sett inneholder disse rettsaktene bestemmelser om at privatpersoner har rett til å bli underrettet om årsakene som ligger til grunn for en avgjørelse (f.eks. avslag på en søknad om kreditt), til å bestride ufullstendige eller uriktige opplysninger (samt bruk av ulovlige faktorer) og til å klage. Disse reglene sikrer vern i det trolig relativt begrensede antallet tilfeller der automatiserte avgjørelser vil bli truffet av Privacy Shield-organisasjonen selv([24]). Med tanke på den økende bruken i den moderne digitale økonomien av automatisert behandling (herunder profilering) som grunnlag for å treffe avgjørelser som påvirker privatpersoner, er dette imidlertid et område som må overvåkes nøye. For å lette denne overvåkingen er man kommet til enighet med amerikanske myndigheter om å drøfte automatiserte avgjørelser, herunder likhetene i og forskjellene mellom EUs og De forente staters tilnærming på dette området, i forbindelse med den første årlige gjennomgåelsen samt etterfølgende gjennomgåelser dersom det er relevant.

([20]) Dette gjelder for alle dataoverføringer som utføres innenfor rammene av Privacy Shield-ordningen, herunder opplysninger som er samlet inn i forbindelse med et arbeidsforhold. En egensertifisert amerikansk organisasjon kan i prinsippet bruke opplysninger om menneskelige ressurser for andre formål som ikke gjelder arbeidsforholdet (f.eks. i forbindelse med visse markedsføringsformål), men den må respektere forbudet mot uforenlig behandling, og en slik bruk må bare finne sted i samsvar med prinsippene om opplysningsplikt og valgmulighet. For den amerikanske organisasjonen er det forbudt å straffe en ansatt for å ha benyttet seg av en slik valgmulighet, herunder å begrense den ansattes karrieremuligheter, og dette sikrer at den ansatte til tross for den underordnede stillingen og avhengighetsforholdet, ikke er underlagt press og dermed kan treffe et reelt fritt valg.

([21]) Se vedlegg II avsnitt III nr. 12.

([22]) Se også det supplerende prinsippet om innsyn (vedlegg II avsnitt III nr. 8).

([23]) Se f.eks. Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (FRCA, 15 USC § 1681 et seq.) eller Fair Housing Act (FHA, 42 U.S.C. 3601 et seq.).

([24]) Ved overføring av personopplysninger som er samlet inn i EU, vil avtaleforholdet med privatpersonen (kunden) i de fleste tilfeller være med – og derfor vil enhver avgjørelse basert på automatisert behandling vanligvis bli truffet av – den behandlingsansvarlige i EU som plikter å overholde EUs regelverk om vern av personopplysninger. Dette omfatter også tilfeller der behandlingen utføres av en Privacy Shield-organisasjon som fungerer som representant på vegne av den behandlingsansvarlige i EU.

26) I henhold til prinsippet om *klageadgang, håndheving og ansvar*([25]) skal deltakende organisasjoner sørge for robuste mekanismer for å sikre at de overholder de andre prinsippene samt sikrer klageadgang for registrerte i EU som har fått sine personopplysninger behandlet i strid med prinsippene, herunder effektive rettsmidler. Dersom en organisasjon frivillig har besluttet å foreta egensertifisering([26]) i henhold til Privacy Shield-avtalen mellom EU og De forente stater, plikter den å følge prinsippene. For fortsatt å kunne motta personopplysninger fra Unionen innenfor rammen av Privacy Shield-ordningen skal organisasjonen årlig foreta en ny sertifisering som bekrefter at den deltar i ordningen. Organisasjoner må også treffe tiltak for å kontrollere([27]) at deres offentliggjorte personvernprogrammer er i samsvar med prinsippene og rent faktisk overholdes. Dette kan gjøres enten gjennom et egenvurderingssystem, som skal omfatte interne prosedyrer som sikrer at ansatte får opplæring om gjennomføringen av organisasjonens personvernprogrammer, samt at det foretas en regelmessig og objektiv kontroll av at de overholdes, eller ved eksterne kontroller som kan omfatte revisjon eller stikkprøvekontroller. Organisasjonen må også innføre en effektiv mekanisme for håndtering av eventuelle klager (se også betraktning 43) og skal være underlagt undersøkelses- og håndhevingsmyndigheten som er gitt FTC, det amerikanske transportdepartementet eller andre amerikanske offisielle organer, og som vil sikre en effektiv overholdelse av prinsippene.

27) Det gjelder særlige regler for såkalte «videreoverføringer», dvs. overføring av personopplysninger fra en organisasjon til en tredjepart (behandlingsansvarlig eller databehandler), uavhengig av om denne er plassert i De forente stater eller i en tredjestat utenfor De forente stater (og Unionen). Formålet med disse reglene er å sikre at det vernet av personopplysninger som registrerte i EU garanteres, ikke undergraves og ikke kan omgås ved å overføre opplysningene til tredjeparter. Dette er særlig relevant i de mer komplekse behandlingskjedene som kjennetegner dagens digitale økonomi.

28) I henhold til *prinsippet om ansvar for videreoverføring*([28]) kan en videreoverføring bare skje i) for begrensede og spesifikke formål, ii) med hjemmel i en avtale (eller en sammenlignbar ordning i et konsern([29])) og iii) bare dersom nevnte avtale gir det samme beskyttelsesnivået som det prinsippene gir, herunder kravet om at anvendelsen av prinsippene bare kan begrenses i den grad det er nødvendig av hensyn til nasjonal sikkerhet, rettshåndheving og andre formål i allmennhetens interesse([30]). Dette bør ses i sammenheng med *prinsippet om opplysningsplikt* og, ved videreoverføring til en behandlingsansvarlig tredjepart([31]), med *prinsippet om valgmulighet* som innebærer at registrerte må informeres (blant annet) om typen av / identiteten til en mottakende tredjepart, formålet med videreoverføringen samt muligheten til å motsette seg (reservere seg mot) nevnte overføring eller, når det gjelder sensitive opplysninger, å gi sitt «uttrykkelige samtykke» til videreoverføring. Med hensyn til *prinsippet om dataintegritet og formålsbegrensning* innebærer plikten til å sikre det samme beskyttelsesnivået som det prinsippene gir, at en tredjepart bare kan behandle personopplysningene den har fått overført, for formål som ikke er uforenlige med formålene som de opprinnelig ble samlet inn for, eller med formål som privatpersonen senere har godkjent.

29) Plikten til å sikre det samme beskyttelsesnivået som det som kreves i prinsippene, gjelder alle tredjeparter som er involvert i behandlingen av de overførte opplysningene, uavhengig av hvor de befinner seg (i De forente stater eller i en annen tredjestat), samt når den opprinnelige mottakende tredjeparten selv overfører nevnte opplysninger til en annen mottakende tredjepart, f.eks. dersom behandlingen settes ut til en underleverandør. I alle tilfeller skal det i avtalen med den mottakende tredjeparten fastsettes at sistnevnte skal underrette Privacy Shield-organisasjonen dersom den fastslår at den ikke lenger

([25]) Se også det supplerende prinsippet om tvisteløsning og håndheving (vedlegg II avsnitt III nr. 11).
([26]) Se også det supplerende prinsippet om egensertifisering (vedlegg II avsnitt III nr. 6).
([27]) Se også det supplerende prinsippet om kontroll (vedlegg II avsnitt III nr. 7).
([28]) Se også det supplerende prinsippet om obligatoriske avtaler om videreoverføringer (vedlegg II avsnitt III nr. 10).
([29]) Se det supplerende prinsippet om obligatoriske avtaler om videreoverføringer (vedlegg II avsnitt III nr. 10 bokstav b)). Selv om dette prinsippet muliggjør overføringer som også er basert på ikke-kontraktsmessige instrumenter (f.eks. konserninterne overholdelses- og kontrollprogrammer), framgår det klart av teksten at disse instrumentene alltid må «sikre kontinuitet i vernet av personopplysninger i henhold til prinsippene». Ettersom den egensertifiserte amerikanske organisasjonen fortsatt vil være ansvarlig for å overholde prinsippene, vil den også ha et sterkt incitament til å bruke instrumenter som rent faktisk er effektive i praksis.
([30]) Se vedlegg II avsnitt I nr. 5.
([31]) Registrerte vil ikke ha rett til å motsette seg overføring dersom personopplysningene overføres til en tredjepart som fungerer som representant og utfører oppgaver på vegne av og på instruks fra den amerikanske organisasjonen. Dette krever imidlertid at det inngås en avtale med representanten, og at den amerikanske organisasjonen vil bære ansvaret for å sikre det vernet som prinsippene gir, ved å utøve sin instruksmyndighet.

kan oppfylle denne forpliktelsen. Da skal tredjeparten innstille behandlingen eller treffe andre rimelige og hensiktsmessige tiltak for å avhjelpe situasjonen([32]). Dersom det oppstår problemer med overholdelse av prinsippene i (under) leverandørkjeden, skal Privacy Shield-organisasjonen som fungerer som behandlingsansvarlig for personopplysningene, bevise at den ikke er ansvarlig for hendelsen som forvoldte skaden. I motsatt fall skal den påta seg ansvaret i samsvar med *prinsippet om klageadgang, håndheving og ansvar*. Ved videreoverføring til en tredjepart som fungerer som representant, gjelder det ytterligere vern([33]).

2.2. *Åpenhet i, forvaltning av og tilsyn med Privacy Shield-avtalen mellom EU og De forente stater*

30) Privacy Shield-avtalen mellom EU og De forente stater inneholder tilsyns- og håndhevingsmekanismer som gjør det mulig å kontrollere og sikre at amerikanske egensertifiserte selskaper overholder prinsippene, samt at en eventuell manglende overholdelse korrigeres. Disse mekanismene er fastsatt i prinsippene (vedlegg II) og de forpliktende tilsagnene avgitt av det amerikanske handelsdepartementet (vedlegg I), FTC (vedlegg IV) og det amerikanske transportdepartementet (vedlegg V).

31) For å sikre riktig anvendelse av Privacy Shield-avtalen mellom EU og De forente stater skal berørte parter, f.eks. registrerte, opplysningsoverførere og nasjonale personvernmyndigheter, kunne identifisere hvilke organisasjoner som har sluttet seg til prinsippene. I denne forbindelse har det amerikanske handelsdepartementet påtatt seg å føre og offentliggjøre en liste over organisasjoner som ved egensertifisering har sluttet seg til prinsippene, og som er underlagt minst én av håndhevingsmyndighetene omhandlet i vedlegg I og II til denne beslutning («Privacy Shield-listen»)([34]). Handelsdepartementet vil oppdatere listen på grunnlag av en organisasjons årlige anmodninger om ny sertifisering eller dersom en organisasjon trekker seg eller utelukkes fra Privacy Shield-ordningen. Det vil også føre og offentliggjøre en offisiell fortegnelse over organisasjoner som er blitt fjernet fra listen, og i hvert enkelt tilfelle angi årsaken til dette. Det vil dessuten angi en lenke til listen over Privacy Shield-relaterte FTC-håndhevingssaker på FTCs nettsted.

32) Det amerikanske handelsdepartementet vil offentliggjøre både Privacy Shield-listen og anmodningene om ny sertifisering på et eget nettsted. Egensertifiserte organisasjoner må til gjengjeld angi nettadressen til Privacy Shield-listen som forvaltes av departementet. Dersom en organisasjons personvernprogram er tilgjengelig på nettet, skal det inneholde en hyperlenke til Privacy Shield-nettstedet samt en hyperlenke til nettstedet eller klageskjemaet til den uavhengige klagemekanismen med ansvar for å behandle uløste klager. Handelsdepartementet vil i forbindelse med en organisasjons sertifisering og ny sertifisering av sin deltakelse i ordningen foreta en systematisk kontroll av at organisasjonens personvernprogrammer er i samsvar med prinsippene.

33) Organisasjoner som vedvarende ikke overholder prinsippene, vil bli fjernet fra Privacy Shield-listen og skal sende tilbake eller slette personopplysningene de har mottatt innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater. Organisasjoner som fjernes fra listen av andre årsaker, f.eks. organisasjoner som frivillig har besluttet ikke lenger å delta, eller som ikke har foretatt ny sertifisering, kan beholde nevnte opplysninger dersom de årlig bekrefter overfor det amerikanske handelsdepartementet at de fortsatt vil følge prinsippene eller sikrer et tilstrekkelig vern av personopplysningene ved hjelp av andre godkjente midler (f.eks. en avtale som fullt ut gjenspeiler kravene i de relevante standardavtalevilkårene som er godkjent av Kommisjonen). I slike tilfeller skal organisasjonen utpeke et kontaktpunkt i organisasjonen for alle Privacy Shield-relaterte spørsmål.

34) Det amerikanske handelsdepartementet vil overvåke organisasjoner som ikke lenger deltar i Privacy Shield-ordningen, enten fordi de har trukket seg frivillig fra den, eller fordi sertifiseringen er utløpt, for å kontrollere om de akter å sende tilbake, slette eller beholde([35]) personopplysningene som de tidligere har mottatt innenfor rammen av ordningen. Dersom

([32]) Situasjonen varierer avhengig av om tredjeparten er en behandlingsansvarlig eller en databehandler (representant). I det første tilfellet skal det i avtalen med tredjeparten fastsettes at sistnevnte skal innstille behandlingen eller treffe andre rimelige og nødvendige tiltak for å avhjelpe situasjonen. I det andre tilfellet er det Privacy Shield-organisasjonen – som er den organisasjonen som er ansvarlig for behandlingen og gir instrukser til representanten – som skal treffe disse tiltakene.

([33]) I dette tilfellet skal den amerikanske organisasjonen også treffe rimelige og nødvendige tiltak i) for å sikre at representanten behandler personopplysningene som er overført, effektivt og på en måte som er i samsvar med organisasjonens forpliktelser i henhold til prinsippene, og ii) for å stoppe og rette opp uautorisert behandling etter melding om dette.

([34]) Informasjon om forvaltning av Privacy Shield-listen finnes i vedlegg I og II (avsnitt I nr. 3, avsnitt I nr. 4, avsnitt III nr. 6 bokstav d) og avsnitt III nr. 11 bokstav g).

([35]) Se f.eks. vedlegg II avsnitt I nr. 3, avsnitt III nr. 6 bokstav f) og avsnitt III nr. 11 bokstav g) i).

organisasjonene beholder disse opplysningene, skal de fortsatt anvende prinsippene på dem. Dersom handelsdepartementet har fjernet organisasjoner fra ordningen på grunn av vedvarende manglende overholdelse av prinsippene, skal det sikre at disse organisasjonene sender tilbake eller sletter personopplysningene de har mottatt innenfor rammen av ordningen.

35) Dersom en organisasjon av en eller annen grunn trer ut av Privacy Shield-ordningen, skal den fjerne alle offentlige erklæringer som antyder at den fortsatt deltar i eller har rett til å nyte godt av fordelene ved avtalen, særlig enhver henvisning til avtalen i organisasjonens offentliggjorte personvernprogram. Det amerikanske handelsdepartementet vil søke etter og håndtere falske påstander om deltakelse i ordningen, herunder fra tidligere medlemmer([36]). En organisasjon som gir allmennheten uriktige opplysninger om sin tilslutning til prinsippene i form av villedende erklæringer eller praksis, kan bli gjenstand for håndhevingstiltak truffet av FTC, det amerikanske transportdepartementet eller andre relevante amerikanske håndhevingsmyndigheter. Avgivelse av uriktige opplysninger til det amerikanske handelsdepartementet kan medføre rettslig forfølging i henhold til False Statements Act (18 U.S.C. § 1001)([37]).

36) Det amerikanske handelsdepartementet vil *ex officio* undersøke eventuelle falske påstander om deltakelse i Privacy Shield-ordningen eller feilaktig bruk av Privacy Shield-sertifiseringsmerket, og personvernmyndigheter kan henvise organisasjoner til et fast kontaktpunkt i departementet med henblikk på kontroll. Dersom en organisasjon har trukket seg fra Privacy Shield-ordningen, ikke foretar ny sertifisering eller fjernes fra Privacy Shield-listen, vil handelsdepartementet foreta en løpende kontroll av at organisasjonen i sitt offentliggjorte personvernprogram har slettet enhver henvisning til Privacy Shield-ordningen som antyder at organisasjonen fortsatt deltar i den, og dersom organisasjonen fortsetter å framsette falske påstander, henvise saken til FTC, det amerikanske transportdepartementet eller en annen vedkommende myndighet med henblikk på mulige håndhevingstiltak. Departementet vil også sende spørreskjemaer til organisasjoner hvis egensertifisering utløper eller som frivillig har trukket seg fra Privacy Shield-ordningen, for å kontrollere om organisasjonen akter å sende tilbake, slette eller fortsette å anvende personvernprinsippene på personopplysningene den mottok mens den deltok i Privacy Shield-ordningen, og, dersom den akter å beholde personopplysningene, kontrollere hvem i organisasjonen som vil fungere som fast kontaktpunkt for Privacy Shield-relaterte spørsmål.

37) Det amerikanske handelsdepartementet vil *ex officio* løpende kontrollere om egensertifiserte organisasjoner overholder prinsippene([38]), herunder ved å sende detaljerte spørreskjemaer. Det vil også systematisk foreta kontroller dersom det mottar en spesifikk (begrunnet) klage, dersom en organisasjon ikke gir tilfredsstillende svar på departementets forespørsler, eller dersom det foreligger troverdig dokumentasjon som tyder på at en organisasjon ikke overholder prinsippene. Når det er relevant, vil handelsdepartementet også rådføre seg med personvernmyndighetene i forbindelse med nevnte kontroller.

2.3. *Klagemekanismer, klagebehandling og håndheving*

38) I henhold til *prinsippet om klageadgang, håndheving og ansvar* i Privacy Shield-avtalen mellom EU og De forente stater skal organisasjoner sørge for klageadgang for privatpersoner som berøres av manglende overholdelse av prinsippene, noe som gir registrerte i EU mulighet til å klage på egensertifiserte amerikanske selskapers manglende overholdelse av prinsippene, og til å få slike klager løst, ved behov ved hjelp av en avgjørelse om effektive avhjelpende tiltak.

39) Som ledd i egensertifiseringen skal organisasjoner oppfylle kravene i prinsippet om klageadgang, håndheving og ansvar ved å stille til rådighet effektive og lett tilgjengelige uavhengige klagemekanismer som kan undersøke og finne en rask løsning på klager fra privatpersoner eller eventuelle tvister, uten at dette medfører kostnader for den enkelte.

40) Organisasjoner kan velge uavhengige klagemekanismer i enten Unionen eller De forente stater. Dette omfatter også muligheten til frivillig å forplikte seg til å samarbeide med personvernmyndighetene i EU. Denne valgmuligheten

([36]) Se «Søke etter og håndtere falske påstander om deltakelse» i vedlegg I.
([37]) Se vedlegg II avsnitt III nr. 6 bokstav h) og avsnitt III nr. 11 bokstav f).
([38]) Se vedlegg I.

foreligger imidlertid ikke når organisasjoner behandler opplysninger om menneskelige ressurser; i slike tilfeller er det obligatorisk å samarbeide med personvernmyndighetene. Andre alternativer er uavhengig alternativ tvisteløsning eller *personvernprogrammer* utarbeidet i privat sektor der personvernprinsippene er innlemmet. Det sistnevnte må omfatte effektive håndhevingsmekanismer i samsvar med kravene i prinsippet om klageadgang, håndheving og ansvar. Organisasjoner plikter å løse eventuelle problemer med manglende overholdelse av prinsippene. De skal også presisere at de er underlagt undersøkelses- og håndhevingsmyndigheten som er gitt FTC, det amerikanske transportdepartementet eller andre amerikanske offisielle organer.

41) Privacy Shield-ordningen gir dermed registrerte en rekke muligheter til å utøve sine rettigheter, klage på egensertifiserte amerikanske selskapers manglende overholdelse av prinsippene og til å få klagene løst, ved behov ved hjelp av en avgjørelse om effektive avhjelpende tiltak. Privatpersoner kan klage direkte til en organisasjon, til et uavhengig tvisteløsningsorgan utpekt av organisasjonen, til nasjonale personvernmyndigheter eller til FTC.

42) Dersom klagene ikke er blitt løst av en av disse klage- eller håndhevingsmekanismene, har privatpersoner også rett til å bringe saken inn for Privacy Shield-panelet med henblikk på tvungen voldgift (vedlegg 1 til vedlegg II til denne beslutning). Med unntak av voldgiftspanelet, som krever at visse andre rettsmidler først skal være uttømt før saken kan bringes inn for det, kan privatpersoner fritt velge å benytte en av eller alle disse klagemekanismene, og de plikter ikke å velge en bestemt mekanisme framfor en annen eller å følge en bestemt rekkefølge. Det anbefales imidlertid å følge den logiske rekkefølgen som er beskrevet nedenfor.

43) For det første kan registrerte i EU klage på manglende overholdelse av prinsippene ved å ta direkte kontakt med det *amerikanske egensertifiserte selskapet*. For å fremme en løsning skal organisasjonen opprette en effektiv klagemekanisme for å behandle slike klager. En organisasjons personvernprogram må derfor inneholde tydelig informasjon om et kontaktpunkt som privatpersoner kan henvende seg til, enten i eller utenfor organisasjonen, som vil stå for behandlingen av klager (herunder enhver relevant virksomhet i Unionen som kan svare på henvendelser eller klager), og om de uavhengige klagebehandlingsmekanismene.

44) Ved mottak av en klage fra en privatperson, direkte fra vedkommende eller via det amerikanske handelsdepartementet som har fått saken henvist fra en personvernmyndighet, skal organisasjonen svare den registrerte i EU innen 45 dager. Svaret skal inneholde en vurdering av om klagen er berettiget, og opplysninger om hvordan organisasjonen vil løse problemet. Organisasjonene plikter også å svare omgående på henvendelser og andre forespørsler om informasjon fra handelsdepartementet eller en personvernmyndighet([39]) (dersom organisasjonen har forpliktet seg til å samarbeide med personvernmyndigheten) som gjelder deres tilslutning til prinsippene. Organisasjonene skal føre protokoll over gjennomføringen av sine personvernprogrammer og på forespørsel gjøre dette tilgjengelig for en uavhengig klagemekanisme eller FTC (eller en annen amerikansk myndighet med kompetanse til å undersøke urimelig og villedende praksis) i forbindelse med en undersøkelse av eller en klage på manglende overholdelse.

45) For det andre kan en person også klage direkte til *det uavhengige tvisteløsningsorganet* (enten i De forente stater eller i Unionen) som en organisasjon har utpekt med henblikk på å undersøke og løse individuelle klager (med mindre de er åpenbart uberettigede eller grunnløse), og for å sikre egnet gratis klageadgang for privatpersoner. De sanksjonene og korrigerende tiltakene som et slikt organ pålegger, skal være tilstrekkelig strenge til å sikre at organisasjonene overholder prinsippene, og bør sikre at organisasjonen utbedrer eller retter opp følgene av den manglende overholdelsen og, avhengig av omstendighetene, avslutter den videre behandlingen av de aktuelle personopplysningene og/eller sletter dem, og at den manglende overholdelsen som er konstatert, offentliggjøres. De uavhengige tvisteløsningsorganene som en organisasjon har utpekt, skal på sine offentlige nettsteder legge ut relevant informasjon om Privacy Shield-avtalen mellom EU og De forente stater og de tjenestene de yter innenfor rammen av den. De skal hvert år offentliggjøre en årlig rapport med aggregert statistikk over disse tjenestene([40]).

([39]) Dette er myndigheten med ansvar for håndteringen utpekt av panelet av personvernmyndigheter fastsatt i det supplerende prinsippet om personvernmyndighetenes rolle (vedlegg II avsnitt III nr. 5).

([40]) Den årlige rapporten skal inneholde 1) informasjon om det samlede antallet Privacy Shield-relaterte klager som er mottatt i rapporteringsåret, 2) typen klager som er mottatt, 3) kvalitetsindikatorer for tvisteløsning, f.eks. klagebehandlingstid, og 4) utfallet av de mottatte klagene, særlig antall og typer pålagte korrigerende tiltak eller sanksjoner.

46) Det amerikanske handelsdepartementet vil som et ledd i sine kontroller av at prinsippene overholdes, kontrollere at egensertifiserte amerikanske selskaper faktisk har registrert seg ved de uavhengige klagemekanismene de hevder å ha registrert seg ved. Både organisasjonene og de ansvarlige uavhengige klagemekanismene skal omgående svare på henvendelser og forespørsler fra handelsdepartementet om informasjon knyttet til Privacy Shield-ordningen.

47) Dersom en organisasjon ikke etterkommer en avgjørelse truffet av et tvisteløsningsorgan eller et selvreguleringsorgan, skal disse organene melde dette til det amerikanske handelsdepartementet og FTC (eller en annen amerikansk myndighet med kompetanse til å undersøke tilfeller av urimelig eller villedende praksis) eller en vedkommende domstol([41]). Dersom en organisasjon nekter å etterkomme en endelig avgjørelse fra et selvreguleringsorgan, et uavhengig tvisteløsningsorgan eller et offentlig organ på personvernområdet, eller dersom et slikt organ fastslår at en organisasjon gjentatte ganger ikke overholder prinsippene, vil dette bli ansett som en vedvarende manglende overholdelse som vil føre til at handelsdepartementet, etter først å ha gitt den aktuelle organisasjonen 30 dagers varsel og mulighet til å svare, vil fjerne organisasjonen fra listen([42]). Dersom organisasjonen etter å ha blitt fjernet fra listen fastholder at den er Privacy Shield-sertifisert, vil handelsdepartementet henvise saken til FTC eller et annet håndhevingsorgan([43]).

48) For det tredje kan en privatperson også inngi klage til en nasjonal *personvernmyndighet*. Organisasjoner plikter å samarbeide med personvernmyndigheten i forbindelse med undersøkelse og avgjørelse av klager, enten når det gjelder behandling av opplysninger om menneskelige ressurser som er samlet inn i forbindelse med et arbeidsforhold, eller når den aktuelle organisasjonen frivillig har underlagt seg personvernmyndighetenes tilsyn. Organisasjoner skal særlig svare på henvendelser, rette seg etter anbefalinger fra personvernmyndigheten, herunder om utbedringstiltak, og bekrefte skriftlig overfor personvernmyndigheten at nevnte tiltak er truffet.

49) Personvernmyndighetenes anbefalinger vil bli formidlet gjennom et uformelt panel av personvernmyndigheter etablert på unionsplan([44]), noe som vil bidra til å sikre en harmonisert og sammenhengende tilnærming til en bestemt klage. Det vil bli utstedt anbefalinger etter at begge parter i tvisten har hatt en rimelig mulighet til å kommentere og legge fram eventuell dokumentasjon som de mener er relevant. Panelet vil utstede anbefalinger så snart kravet om behørig behandling tillater det, og som en alminnelig regel innen 60 dager etter at en klage er mottatt. Dersom en organisasjon ikke har etterkommet anbefalingen innen 25 dager etter at den ble gitt, og ikke har gitt en tilfredsstillende forklaring på årsaken til dette, vil panelet meddele at det enten akter å oversende saken til FTC (eller en annen vedkommende amerikansk håndhevingsmyndighet) eller konkludere med at det har skjedd et alvorlig brudd på plikten til å samarbeide. I det første alternativet kan dette føre til håndhevingstiltak basert på avsnitt 5 i FTC Act (eller tilsvarende lovgivning). I det andre alternativet vil panelet underrette det amerikanske handelsdepartementet som vil anse organisasjonens manglende vilje til å etterkomme panelets anbefalinger, som en vedvarende manglende overholdelse av prinsippene, noe som vil medføre at organisasjonen fjernes fra Privacy Shield-listen.

50) Dersom personvernmyndigheten som klagen er rettet til, ikke har truffet eller ikke har truffet tilstrekkelige tiltak for å behandle klagen, har den enkelte klager mulighet til å bringe saken inn for de nasjonale domstolene i den berørte medlemsstaten.

51) Privatpersoner kan dessuten inngi klage til personvernmyndighetene også når panelet av personvernmyndigheter ikke er utpekt som en organisasjons tvisteløsningsorgan. I disse tilfellene kan personvernmyndigheten henvise slike klager til enten det amerikanske handelsdepartementet eller til FTC. For å fremme og styrke samarbeidet i spørsmål som gjelder individuelle klager og Privacy Shield-organisasjoners manglende overholdelse av prinsippene, vil handelsdepartementet opprette et fast kontaktpunkt som skal fungere som bindeledd og bistå personvernmyndighetene i deres undersøkelser av om en organisasjon overholder prinsippene([45]). FTC har dessuten forpliktet seg til å opprette et fast kontaktpunkt([46]) og bistå personvernmyndighetene med undersøkelser i henhold til U.S. SAFE WEB Act([47]).

([41]) Se vedlegg II avsnitt III nr. 11 bokstav e).
([42]) Se vedlegg II avsnitt III nr. 11 bokstav g), særlig punkt ii) og iii).
([43]) Se «Søke etter og håndtere falske påstander om deltakelse» i vedlegg I.
([44]) Personvernmyndighetene bør fastsette forretningsordenen for det uformelle panelet av personvernmyndigheter på grunnlag av deres kompetanse til å organisere sitt arbeid og samarbeide med hverandre.
([45]) Se «Øke samarbeidet med personvernmyndighetene» og «Tiltak for å gjøre det enklere å avgjøre klager på manglende overholdelse» i vedlegg I samt vedlegg II avsnitt II nr. 7 bokstav e).
([46]) Se vedlegg IV, s. 6.
([47]) Ibid.

52) For det fjerde har det amerikanske *handelsdepartementet* forpliktet seg til å motta, gjennomgå og gjøre sitt beste for å avgjøre klager på en organisasjons manglende overholdelse av prinsippene. Handelsdepartementet har i denne forbindelse utarbeidet særskilte framgangsmåter som personvernmyndighetene skal følge for å henvise klager til et fast kontaktpunkt, spore klagene og følge opp selskaper for å fremme en løsning. For å framskynde behandlingen av individuelle klager skal kontaktpunktet ha direkte kontakt med den berørte personvernmyndigheten i saker som gjelder manglende overholdelse av prinsippene, og særlig underrette myndigheten om statusen for klagene senest 90 dager etter henvisningen. Dette gir registrerte mulighet til å klage på amerikanske egensertifiserte selskaper som ikke overholder prinsippene, direkte til sin nasjonale personvernmyndighet og å få klagene kanalisert til det amerikanske handelsdepartementet, som er den myndigheten i De forente stater som forvalter Privacy Shield-avtalen mellom EU og De forente stater. Handelsdepartementet har også forpliktet seg til å legge fram en rapport med en analyse i aggregert form av klagene den mottar hvert år, i forbindelse med den årlige gjennomgåelsen av hvordan Privacy Shield-avtalen mellom EU og De forente stater fungerer([48]).

53) Dersom det amerikanske handelsdepartementet på grunnlag av sine *ex officio*-kontroller, klager eller annen informasjon konkluderer med at en organisasjon vedvarende har unnlatt å overholde personvernprinsippene, vil nevnte organisasjon bli fjernet fra Privacy Shield-listen. Dersom en organisasjon nekter å etterkomme en endelig avgjørelse truffet av et selvreguleringsorgan, et uavhengig tvisteløsningsorgan eller et offentlig organ på personvernområdet, herunder en personvernmyndighet, vil det bli ansett som en vedvarende manglende overholdelse av prinsippene.

54) For det femte skal en Privacy Shield-organisasjon være underlagt undersøkelses- og håndhevingsmyndigheten som innehas av amerikanske myndigheter, særlig *Federal Trade Commission*([49]), noe som vil sikre en effektiv overholdelse av prinsippene. FTC vil prioritere saker som gjelder manglende overholdelse av personvernprinsippene, og som den får henvist fra uavhengige tvisteløsningsorganer eller selvreguleringsorganer, det amerikanske handelsdepartementet og personvernmyndigheter (som handler på eget initiativ eller som følge av klager), for å bestemme om det foreligger et brudd på avsnitt 5 i FTC Act([50]). FTC har forpliktet seg til å utarbeide en standardisert henvisningsprosess, til å utpeke et kontaktpunkt for henvisninger fra personvernmyndighetene og til å utveksle informasjon om henvisninger. FTC vil dessuten akseptere klager direkte fra privatpersoner og på eget initiativ undersøke spørsmål knyttet til Privacy Shield-ordningen, særlig som et ledd i sine mer generelle undersøkelser av personvernspørsmål.

55) FTC kan håndheve overholdelsen av prinsippene gjennom forliksavgjørelser («*consent orders*») og vil systematisk kontrollere at nevnte avgjørelser overholdes. Ved manglende overholdelse fra en organisasjon kan FTC henvise saken til vedkommende domstol med henblikk på å ilegge sivilrettslige sanksjoner eller pålegge andre korrigerende tiltak, herunder for enhver skade forårsaket av den ulovlige praksisen. FTC kan alternativt anmode en føderal domstol om å utstede en midlertidig eller permanent forføyning eller andre rettslige tiltak. Enhver forliksavgjørelse som utstedes til en Privacy Shield-organisasjon, vil inneholde bestemmelser om egenrapportering([51]), og organisasjoner plikter å offentliggjøre alle relevante Privacy Shield-relaterte avsnitt i alle overholdelses- eller vurderingsrapporter som legges fram for FTC. FTC vil dessuten føre en nettbasert liste over selskaper som omfattes av FTC-avgjørelser eller rettsavgjørelser i Privacy Shield-saker.

56) For det sjette kan registrerte i EU som en siste utvei dersom ingen av de andre tilgjengelige klagemulighetene har ført til at klagen er avgjort på en tilfredsstillende måte, bringe saken inn for «*Privacy Shield-panelet*» med henblikk på tvungen voldgift. Organisasjoner skal underrette registrerte om at de på visse vilkår har mulighet til å få saken løst ved tvungen voldgift, og når en registrert har underrettet en organisasjon om at vedkommende har valgt denne muligheten, plikter den berørte organisasjonen å svare([52]).

([48]) Se «Tiltak for å gjøre det enklere å avgjøre klager på manglende overholdelse» i vedlegg I.

([49]) En Privacy Shield-organisasjon skal offentlig erklære at den forplikter seg til å overholde prinsippene samt offentliggjøre sine personvernprogrammer i tråd med disse prinsippene og gjennomføre dem fullt ut. Manglende overholdelse kan håndheves i henhold til avsnitt 5 i FTC Act som forbyr urimelig eller villedende atferd i forbindelse med handel.

([50]) Ifølge informasjon fra FTC har FTC ikke myndighet til å foreta stedlige tilsyn på området personvern. FTC har imidlertid myndighet til å tvinge organisasjoner til å legge fram dokumenter og vitneutsagn (se avsnitt 20 i FTC Act) og kan bruke domstolsapparatet for å få håndhevet slike pålegg i tilfelle manglende overholdelse.

([51]) FTC-avgjørelser eller rettsavgjørelser kan kreve at selskaper iverksetter personvernprogrammer og regelmessig gjør overholdelsesrapporter eller vurderinger av nevnte programmer som er foretatt av en uavhengig tredjepart, tilgjengelige for FTC.

([52]) Se vedlegg II avsnitt II nr. 1 punkt xi) og avsnitt III nr. 7 bokstav c).

57) Voldgiftspanelet vil bestå av en gruppe på minst 20 voldgiftsmenn utpekt av det amerikanske handelsdepartementet og Kommisjonen på grunnlag av disse personenes uavhengighet, integritet og erfaring med De forente staters personvernlovgivning og Unionens regelverk for vern av personopplysninger. For hver tvist skal partene opprette et panel bestående av en eller tre([53]) voldgiftsmenn fra denne gruppen. Voldgiftsprosedyren skal være underlagt standard voldgiftsregler som skal fastsettes av handelsdepartementet og Kommisjonen i fellesskap. Disse reglene vil supplere den allerede fastsatte ordningen som inneholder flere elementer som gjør denne mekanismen mer tilgjengelig for registrerte i EU: i) ved forberedelse av en klage for panelet kan den registrerte få hjelp av sin nasjonale personvernmyndighet, ii) voldgiftsbehandlingen vil finne sted i De forente stater, men registrerte i EU kan velge å delta ved hjelp av video- eller telefonkonferanse uten ekstra omkostninger for privatpersonen, iii) voldgiftsbehandlingen vil som en regel foregå på engelsk, men den registrerte vil på begrunnet anmodning normalt([54]) ha tilgang til tolking under voldgiftsbehandlingen samt oversettelse uten ekstra omkostninger for vedkommende, og iv) hver part skal bære sine egne advokatkostnader dersom parten møter med advokat for panelet, men handelsdepartementet vil opprette et fond som finansieres ved årlige bidrag fra Privacy Shield-organisasjonene, og som skal dekke de støtteberettigede voldgiftskostnadene opp til et maksimumsbeløp som skal fastsettes av amerikanske myndigheter i samråd med Kommisjonen.

58) Privacy Shield-panelet har myndighet til å pålegge «rimelige individuelle og ikke-økonomiske tiltak» («individual-specific, non-monetary equitable relief»)([55]) som er nødvendige for å korrigere den manglende overholdelsen av prinsippene. Selv om panelet vil ta hensyn til andre korrigerende tiltak som allerede er iverksatt gjennom andre Privacy Shield-mekanismer når det treffer sine avgjørelser, kan en privatperson fremdeles velge å bringe saken inn for voldgift dersom vedkommende mener at disse andre tiltakene ikke er tilstrekkelige. Registrerte i EU kan dermed kreve saken avgjort ved voldgift dersom tiltak eller manglende tiltak fra vedkommende amerikanske myndigheter (f.eks. FTC) ikke har ført til at deres klager er blitt avgjort på en tilfredsstillende måte. En sak kan ikke bringes inn for voldgift dersom en personvernmyndighet har rettslig myndighet til å avgjøre den aktuelle klagen på det amerikanske egensertifiserte selskapet, nærmere bestemt i tilfeller der organisasjonen enten er forpliktet til å samarbeide med personvernmyndighetene og rette seg etter deres anbefalinger om behandling av opplysninger om menneskelige ressurser som samles inn i forbindelse med et arbeidsforhold, eller frivillig har forpliktet seg til å gjøre dette. Privatpersoner kan få fullbyrdet voldgiftsavgjørelsen ved amerikanske domstoler i henhold til Federal Arbitration Act, noe som sikrer tilgang til rettsmidler dersom et selskap ikke overholder prinsippene.

59) For det sjuende kan det i tilfeller der en organisasjon ikke oppfyller sin plikt til å overholde prinsippene og sitt offentliggjorte personvernprogram, finnes andre muligheter for rettslig prøving i de enkelte amerikanske delstaters lovgivning, som inneholder bestemmelser om rettsmidler under erstatningsretten, og i tilfeller av avgivelse av uriktige opplysninger, urimelig og villedende atferd eller praksis eller avtalebrudd.

60) Dersom en personvernmyndighet etter å ha mottatt en klage fra en registrert i EU anser at overføringen av en persons personopplysninger til en organisasjon i De forente stater skjer i strid med EUs regelverk for vern av personopplysninger, herunder dersom opplysningsoverføreren i EU har grunn til å tro at organisasjonen ikke overholder prinsippene, kan den også utøve sin myndighet overfor opplysningsoverføreren og ved behov gi pålegg om å innstille overføringen av opplysninger.

61) På grunnlag av informasjonen i dette avsnittet anser Kommisjonen at prinsippene utstedt av det amerikanske handelsdepartementet sikrer et nivå for vern av personopplysninger som i hovedtrekk tilsvarer det som garanteres ved de vesentlige grunnleggende prinsippene fastsatt i direktiv 95/46/EF.

62) En effektiv anvendelse av prinsippene er dessuten garantert ved kravene til åpenhet samt det amerikanske handelsdepartementets forvaltning og kontroll av at Privacy Shield-ordningen overholdes.

63) Kommisjonen mener videre at mekanismene for tilsyn, klageadgang og håndheving i Privacy Shield-ordningen gjør det mulig å identifisere Privacy Shield-organisasjoners manglende overholdelse av prinsippene og å straffe disse i praksis samt sikre de registrerte rettsmidler slik at de kan få innsyn i personopplysninger som gjelder dem, og få rettet eller slettet slike opplysninger.

([53]) Antall voldgiftsmenn i panelet skal avtales mellom partene.

([54]) Panelet kan imidlertid beslutte at dekning av kostnadene vil medføre uberettigede eller uforholdsmessige kostnader i den aktuelle voldgiftssaken.

([55]) Privatpersoner kan ikke kreve skadeserstatning i voldgiftssaker, men selv om de krever voldgiftsbehandling, kan de fortsatt kreve skadeserstatning ved de ordinære amerikanske domstolene.

3. AMERIKANSKE OFFENTLIGE MYNDIGHETERS TILGANG TIL OG BRUK AV PERSONOPPLYSNINGER OVERFØRT INNENFOR RAMMEN AV PRIVACY SHIELD-AVTALEN MELLOM EU OG DE FORENTE STATER

64) Slik det framgår av avsnitt I nr. 5 i vedlegg II er overholdelse av prinsippene begrenset til det som er nødvendig for å oppfylle krav knyttet til nasjonal sikkerhet, allmennhetens interesse eller rettshåndheving.

65) Kommisjonen har vurdert begrensningene og garantiene som foreligger i amerikansk rett med hensyn til amerikanske myndigheters tilgang til og bruk av personopplysninger overført innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater for formål knyttet til nasjonal sikkerhet, rettshåndheving og andre formål i allmennhetens interesse. Den amerikanske regjering har via Office of the Director of National Intelligence (ODNI)([56]) også framlagt detaljerte redegjørelser og forpliktende tilsagn for Kommisjonen som er angitt i vedlegg VI til denne beslutning. Ved brev underskrevet av den amerikanske utenriksministeren vedlagt som vedlegg III til denne beslutning har den amerikanske regjering også forpliktet seg til å opprette en ny tilsynsmekanisme for inngrep knyttet til nasjonal sikkerhet, Privacy Shield-ombudet, som skal være uavhengig av etterretningssamfunnet. En redegjørelse fra det amerikanske justis-departementet angitt i vedlegg VII til denne beslutning beskriver begrensningene og garantiene som gjelder for offentlige myndigheters tilgang til og bruk av opplysninger for formål knyttet til rettshåndheving og andre formål i allmennhetens interesse. For å øke åpenheten og gjenspeile nevnte forpliktende tilsagns rettslige art vil hvert av dokumentene som er omhandlet og vedlagt denne beslutning, bli offentliggjort i De forente staters *Federal Register*.

66) Nedenfor redegjøres det nærmere for Kommisjonens konklusjoner om hvilke begrensninger som gjelder for amerikanske offentlige myndigheters tilgang til og bruk av personopplysninger som er overført fra EU til De forente stater, samt forekomsten av et effektivt rettslig vern.

3.1. *Amerikanske offentlige myndigheters tilgang til og bruk av personopplysninger for formål knyttet til nasjonal sikkerhet*

67) Kommisjonens analyse viser at amerikansk rett inneholder en rekke begrensninger når det gjelder tilgang til og bruk av personopplysninger som overføres innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater for formål knyttet til nasjonal sikkerhet, samt tilsyns- og klagemekanismer som i tilstrekkelig grad garanterer at nevnte opplysninger omfattes av et effektivt vern mot ulovlige inngrep og risikoen for misbruk([57]). Siden 2013, da Kommisjonen utstedte sine to meldinger (se betraktning 7), har denne rettslige rammen blitt betraktelig styrket som beskrevet nedenfor.

3.1.1. Begrensninger

68) I henhold til den amerikanske grunnloven er det presidenten, i egenskap av å være øverstkommanderende og regjeringssjef, som har ansvar for den nasjonale sikkerheten og, med hensyn til utenlandsetterretning, å føre De forente staters utenrikspolitikk([58]). Selv om Kongressen har myndighet til å pålegge begrensninger og har gjort dette i forskjellige henseender, kan presidenten innenfor disse grensene styre aktivitetene til det amerikanske etterretningssamfunnet, særlig gjennom presidentordrer («executive orders») eller presidentdirektiver («presidential directives»). Dette gjelder selvfølgelig også på de områdene der det ikke foreligger retningslinjer fra Kongressen. På det nåværende tidspunkt er de to sentrale rettslige instrumentene på dette området en presidentordre, Executive Order 12333 («E.O. 12333»)([59]), og et presidentdirektiv, Presidential Policy Directive 28.

([56]) Direktøren for National Intelligence (DNI) fungerer som leder for det amerikanske etterretningssamfunnet og som hovedrådgiver for presidenten og National Security Council. Se Intelligence Reform and Terrorism Prevention Act fra 2004, Pub. L. 108-458 av 17.12.2004. ODNI fastsetter blant annet kravene til og forvalter og styrer det amerikanske etterretningssamfunnets oppgaver, innsamling, analysering, produksjon og spredning av nasjonal etterretning, herunder ved å utarbeide retningslinjer for tilgang til, bruk og utveksling av informasjon eller etterretning. Se avsnitt 1.3 (a), (b) i E.O. 12333.

([57]) Se Schrems, nr. 91.

([58]) Den amerikanske grunnlov, artikkel II. Se også innledningen til PPD-28.

([59]) E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8. desember 1981). I den grad en presidentordre er offentlig tilgjengelig, definerer den målene, retningen, oppgavene og ansvarsområdene for den amerikanske etterretningsinnsatsen (herunder rollen til de forskjellige enhetene innen etterretningssamfunnet) og fastsetter de generelle parametrene for gjennomføringen av etterretningsaktiviteter (især behovet for å fastsette særlige prosedyreregler). I henhold til avsnitt 3.2 i E.O. 12333 skal presidenten med støtte fra National Security Council og DNI utstede de direktivene, prosedyrene og retningslinjene som er nødvendige for å gjennomføre ordren.

69) Presidential Policy Directive 28 («PPD-28») utstedt 17. januar 2014 inneholder en rekke begrensninger når det gjelder «signaletterretningsoperasjoner»([60]). Dette presidentdirektivet er bindende for amerikanske etterretningsmyndigheter([61]) og vil fortsatt gjelde etter et regjeringsskifte i De forente stater([62]). PPD-28 er særlig viktig for ikke-amerikanske personer, herunder registrerte i EU. I direktivet fastslås det bl.a. følgende:

a) Innsamlingen av signaletterretning skal være hjemlet i lov eller skje med presidentens tillatelse og skal foretas i samsvar med den amerikanske grunnloven (særlig fjerde grunnlovstillegg) og amerikansk rett.

b) Alle personer bør behandles med verdighet og respekt, uavhengig av deres statsborgerskap eller bosted.

c) Alle personer har berettigede personverninteresser når det gjelder behandlingen av deres personopplysninger.

d) Hensynet til personvern og borgerlige frihetsrettigheter skal utgjøre en vesentlig del ved planleggingen av amerikanske signaletterretningsaktiviteter.

e) Amerikanske signaletterretningsaktiviteter skal derfor inneholde tilstrekkelige garantier for personopplysningene til alle privatpersoner, uavhengig av deres statsborgerskap eller bosted.

70) I henhold til PPD-28 kan signaletterretning utelukkende samles inn for formål knyttet til utenlandsetterretning eller kontraspionasje for å støtte nasjonale eller departementale oppgaver, og ikke for noen andre formål (f.eks. for å gi amerikanske selskaper et konkurransefortrinn). ODNI forklarer i denne forbindelse at enhetene innen etterretningssamfunnet «bør stille krav om at innsamlingen, når det er praktisk mulig, bør rettes mot spesifikke utenlandske etterretningsmål eller -emner ved bruk av diskriminanter (f.eks. bestemte fasiliteter, utvalgskriterier og identifikatorer)»([63]). I redegjørelsene gis det også forsikringer om at avgjørelser om innsamling av etterretning ikke overlates til privatpersoner i etterretningssamfunnet, men er underlagt de retningslinjene og prosedyrene som de forskjellige enhetene innen det amerikanske etterretningssamfunnet (byråer) plikter å innføre med henblikk på gjennomføring av PPD-28([64]). Utvikling og valg av egnede utvalgskriterier finner derfor sted innenfor rammen av det overordnede «National Intelligence Priorities Framework» (NIPF) som sikrer at etterretningsprioriteringene fastsettes av beslutningstakere på høyt nivå, og at de gjennomgås regelmessig, slik at de er tilpasset de faktiske truslene for den nasjonale sikkerhet, og samtidig tar hensyn til mulige risikoer, herunder risikoer knyttet til personvern([65]). På grunnlag av dette utvikler og identifiserer personell i de forskjellige byråene spesifikke utvalgskriterier som det antas vil føre til innsamling av utenlandsetterretning som samsvarer med prioriteringene([66]). Utvalgskriteriene må gjennomgås regelmessig for å kontrollere at de fremdeles gir verdifull etterretning i tråd med prioriteringene([67]).

([60]) I henhold til E.O. 12333 er direktøren for National Security Agency (NSA) den funksjonelle lederen for signaletterretning og skal styre en enhetlig organisasjon for signaletterretningsaktiviteter.

([61]) Når det gjelder definisjonen av termen «etterretningssamfunn», se avsnitt 3.5 (h) i E.O. 12333 sammenholdt med n. 1 i PPD-28.

([62]) Se memorandum fra det amerikanske justisdepartementets Office of Legal Counsel til president Clinton 29. januar 2000. Ifølge denne rettslige uttalelsen har et presidentdirektiv de «samme vesentlige rettsvirkninger som en presidentordre».

([63]) ODNIs redegjørelser (vedlegg VI), s. 3.

([64]) Se avsnitt 4 (b) og (c) i PPD-28. Ifølge offentlig tilgjengelig informasjon ble de seks eksisterende formålene bekreftet ved gjennomgåelsen i 2015. Se ODNI, Signals Intelligence Reform, 2016 Progress Report.

([65]) ODNIs redegjørelser (vedlegg VI), s. 6 (med henvisning til Intelligence Community Directive 204). Se også avsnitt 3 i PPD-28.

([66]) ODNIs redegjørelser (vedlegg VI), s. 6. Se f.eks. NSA Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7. oktober 2014. Se også ODNI Status Report 2014. Med hensyn til anmodninger om innsyn i henhold til avsnitt 702 i FISA omfattes anmodninger av de FISC-godkjente minimeringsprosedyrene. Se NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. april 2014.

([67]) Se Signal Intelligence Reform, 2015 Anniversary Report. Se også ODNIs redegjørelser (vedlegg VI), s. 6, 8–9, 11.

71) Kravene i PPD-28 om at innsamling av etterretning alltid skal([68]) være «så målrettet som mulig», og om at etterretningssamfunnet skal prioritere annen tilgjengelig informasjon og egnede og mulige alternativer([69]), er dessuten et uttrykk for en alminnelig regel som går ut på å prioritere målrettet innsamling framfor masseinnsamling. Ifølge garantien fra ODNI sikrer det særlig at masseinnsamling verken er «massiv» eller «vilkårlig», og at unntaket ikke erstatter regelen([70]).

72) Selv om det i PPD-28 forklares at enheter innen etterretningssamfunnet noen ganger må foreta masseinnsamling av signaletterretning i visse situasjoner, f.eks. for å identifisere og vurdere nye eller framvoksende trusler, er enhetene pålagt å prioritere alternativer som gjør det mulig å foreta målrettet signaletterretning([71]). Dette gjør at masseinnsamling bare foretas når målrettet innsamling ved bruk av diskriminanter – dvs. en identifikator knyttet til et bestemt mål (f.eks. målets e-postadresse eller telefonnummer) – ikke er mulig «av tekniske eller praktiske hensyn»([72]). Dette gjelder både for måten signaletterretning samles inn på, og for det som faktisk samles inn([72]).

73) Ifølge ODNIs redegjørelser vil etterretningssamfunnet, selv når det ikke kan bruke spesifikke identifikatorer til å målrette innsamlingen, prøve å avgrense innsamlingen «så mye som mulig». For å sikre dette «brukes det filtre og andre tekniske verktøyer for å målrette innsamlingen mot fasiliteter som kan antas å inneholde kommunikasjon av verdi for utenlandsetterretning» (og dermed oppfylle amerikanske beslutningstakeres krav i henhold til prosessen som er beskrevet i betraktning 70). Som en følge av dette vil masseinnsamling bli målrettet på minst to måter: For det første vil dette alltid være knyttet til spesifikke utenlandsetterretningsmål (f.eks. for å innhente signaletterretning om aktivitetene til en terroristgruppe i en bestemt region) og være rettet mot innsamling av kommunikasjon i forbindelse med dette. Ifølge forsikringen fra ODNI kommer dette til uttrykk ved det faktum at «De forente staters signaletterretningsaktiviteter bare berører en brøkdel av den kommunikasjonen som skjer via internett»([73]). For det andre forklares det i ODNIs redegjørelser at filtrene og de andre tekniske verktøyene som brukes, vil bli utformet på en slik måte at innsamlingen blir «så nøyaktig som mulig» for å sikre at mengden ikke-relevante opplysninger» som samles inn, blir så liten som mulig.

74) Selv når De forente stater vurderer at det er nødvendig å foreta masseinnsamling av signaletterretning på vilkårene fastsatt i betraktning 70–73, begrenser PPD-28 bruken av slike opplysninger til en spesifikk liste med seks formål knyttet til nasjonal sikkerhet med henblikk på å ivareta personvernet og de borgerlige frihetsrettighetene til alle personer, uavhengig av deres statsborgerskap eller bosted([74]). Disse tillatte formålene omfatter tiltak for å avdekke og nøytralisere trusler som stammer fra spionasje, terrorisme, masseødeleggelsesvåpen, trusler mot cybersikkerheten, de væpnede styrker eller

([68]) Se ODNIs redegjørelser (vedlegg VI), s. 3.

([69]) Det bør også bemerkes at i henhold til avsnitt 2.4 i E.O. 12333 skal enheter innen etterretningssamfunnet «bruke minst mulig inngripende innsamlingsteknikker i De forente stater». Når det gjelder begrensningene med hensyn til å erstatte masseinnsamling med målrettet innsamling, henvises det til resultatene av en vurdering foretatt av National Research Council i henhold til en rapport fra Den europeiske unions byrå for grunnleggende rettigheter: Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015), s. 18.

([70]) ODNIs redegjørelser (vedlegg VI), s. 4.

([71]) Se også avsnitt 5 (d) i PPD-28 der det fastslås at direktøren for National Intelligence i samarbeid med lederne for de relevante enhetene innen etterretningssamfunnet og Office of Science and Technology Policy skal legge fram for presidenten «en rapport med en vurdering av muligheten for å utvikle en programvare som vil gjøre det lettere for etterretningssamfunnet å foreta målrettet innsamling av opplysninger istedenfor masseinnsamling». Ifølge offentlig tilgjengelig informasjon framgår det av denne rapporten at «det ikke finnes noe programvarebasert alternativ som fullt ut kan erstatte masseinnsamling med henblikk på å avdekke visse trusler mot den nasjonale sikkerhet». Se Signals Intelligence Reform, 2015 Anniversary Report.

([72]) Se fotnote 68.

([73]) ODNIs redegjørelser (vedlegg VI). Dette gjelder særlig bekymringen uttrykt av de nasjonale personvernmyndighetene i deres uttalelse om utkastet til beslutning om tilstrekkelig beskyttelsesnivå. Se artikkel 29-arbeidsgruppen for personvern, uttalelse 1/2016 om Privacy Shield-avtalen mellom EU og De forente stater – utkast til beslutning om tilstrekkelig beskyttelsesnivå (vedtatt 13. april 2016), s. 38 sammenholdt med n. 47.

([74]) Se avsnitt 2 i PPD-28.

militært personell samt tverrnasjonale kriminelle trusler knyttet til de fem andre formålene, og vil bli gjennomgått minst én gang i året. Ifølge redegjørelsene fra den amerikanske regjering har enheter innen etterretningssamfunnet styrket sin analysepraksis og sine analysestandarder for søk i ikke-vurdert signaletterretning, slik at de oppfyller disse kravene. Bruken av målrettede søk «sikrer at analytikere får seg forelagt bare de opplysningene som antas å ha en potensiell etterretningsverdi»([75]).

75) Disse begrensningene er særlig relevante for personopplysninger som overføres innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, særlig dersom innsamling av personopplysninger skal finne sted utenfor De forente stater, herunder mens opplysningene er under overføring via de transatlantiske kablene fra Unionen til De forente stater. Som bekreftet av amerikanske myndigheter i ODNIs redegjørelser får begrensningene og garantiene som angis der, herunder dem som er nevnt i PPD-28, anvendelse på slik innsamling([76]).

76) Selv om disse prinsippene ikke er formulert ved bruk av disse juridiske begrepene, gjenspeiler de det vesentligste i prinsippene om nødvendighet og forholdsmessighet. Målrettet innsamling er en klar prioritering, mens masseinnsamling er begrenset til (unntaks)situasjoner der målrettet innsamling av tekniske eller praktiske årsaker ikke er mulig. Selv når *masseinnsamling* ikke kan unngås, er videre «bruk» av slike opplysninger gjennom tilgang *strengt begrenset* til spesifikke og berettigede formål knyttet til nasjonal sikkerhet([77]).

77) Ettersom et direktiv utstedes av presidenten i egenskap av å være regjeringssjef, er disse kravene bindende for hele etterretningssamfunnet og er blitt ytterligere gjennomført gjennom byråenes regler og framgangsmåter som omgjør de generelle prinsippene til spesifikke retningslinjer for den daglige virksomheten. Selv om Kongressen ikke er bundet av PPD-28, har den også truffet tiltak for å sikre at innsamling av og tilgang til personopplysninger i De forente stater er målrettet og ikke foretas «på et generelt grunnlag».

78) Ifølge tilgjengelig informasjon, herunder redegjørelsene fra den amerikanske regjering, framgår det at når opplysningene er overført til organisasjoner i De forente stater som er egensertifiserte i henhold til Privacy Shield-avtalen mellom EU og De forente stater, kan amerikanske etterretningsbyråer bare([78]) be om tilgang til personopplysninger dersom forespørselen er i samsvar med Foreign Intelligence Surveillance Act (FISA) eller er gjort av Federal Bureau of Investigation (FBI) på grunnlag av et såkalt nasjonalt sikkerhetsbrev («National Security Letter» (NSL))([79]). FISA inneholder flere typer rettslige

([75]) ODNIs redegjørelser (vedlegg VI), s. 4. Se også Intelligence Community Directive 203.

([76]) ODNIs redegjørelser (vedlegg VI), s. 2. Begrensningene fastsatt i E.O. 12333 (f.eks. at innsamlede opplysninger skal være i samsvar med etterretningsprioriteringene fastsatt av presidenten) får også anvendelse.

([77]) Se Schrems, nr. 93.

([78]) FBIs innsamling av opplysninger kan også være basert på rettshåndhevingstillatelser (se avsnitt 3 nr. 2 i denne beslutning).

([79]) Det redegjøres nærmere for bruken av nasjonale sikkerhetsbrev (NSL) i ODNIs redegjørelser (vedlegg VI), s. 13–14 sammenholdt med n. 38. Som angitt i nevnte redegjørelser kan FBI bruke NSL bare for å anmode om innholdsløse opplysninger som er relevante for en godkjent etterforskning knyttet til nasjonal sikkerhet dersom formålet er å beskytte nasjonen mot internasjonal terrorisme eller hemmelige etterretningsaktiviteter. Når det gjelder dataoverføringer innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, er det mest relevante rettslige grunnlaget antagelig Electronic Communications Privacy Act (18 U.S.C. § 2709), der det kreves at det i enhver anmodning om abonnentopplysninger eller transaksjonsregistre skal brukes «et utvalgskriterium som uttrykkelig identifiserer en person, en enhet, et telefonnummer eller en konto».

grunnlag som kan brukes til innsamling (og deretter behandling) av personopplysninger fra registrerte i EU som overføres innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater. Foruten avsnitt 104 i FISA([80]) som omfatter tradisjonell individualisert elektronisk overvåking, og avsnitt 402 i FISA([81]) om installasjon av utstyr for registrering av oppringte numre fra et bestemt telefonnummer («pen register») eller samtalesporingsutstyr («trap and trace»-utstyr), er de to sentrale instrumentene avsnitt 501 i FISA (tidligere avsnitt 215 i U.S. PATRIOT ACT) og avsnitt 702 i FISA([82]).

79) I denne forbindelse forbyr USA FREEDOM Act, som trådte i kraft 2. juni 2015, masseinnsamling av opplysninger basert på avsnitt 402 i FISA («pen register» og «trap and trace»), avsnitt 501 i FISA (tidligere avsnitt 215 i U.S. PATRIOT ACT)([83]) og ved bruk av nasjonale sikkerhetsbrev (NSL), og krever isteden bruk av spesifikke utvalgskriterier («selection terms»([84])).

80) Selv om FISA inneholder ytterligere rettslige grunnlag som tillater at det utføres nasjonale etterretningsaktiviteter, herunder signaletterretning, har Kommisjonens vurdering vist at disse tillatelsene når det gjelder overføring av personopplysninger innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, også begrenser offentlige myndigheters inngrep i målrettet innsamling og tilgang.

81) Dette er helt klart tilfellet når det gjelder tradisjonell individualisert elektronisk overvåking i henhold til avsnitt 104 i FISA([85]). Når det gjelder avsnitt 702 i FISA, som utgjør grunnlaget for to viktige etterretningsprogrammer som drives av de amerikanske etterretningsbyråene (PRISM, UPSTREAM), foretas søk på en målrettet måte ved bruk av individuelle utvalgskriterier som identifiserer spesifikke kommunikasjonselementer, f.eks. målets e-postadresse eller telefonnummer, men ikke stikkord og heller ikke navnene til de berørte privatpersonene([86]). Som påpekt av Privacy and Civil Liberties

([80]) 50 U.S.C. § 1804. Selv om dette rettslige grunnlaget krever at det redegjøres for de faktiske forholdene og omstendighetene som den anmodende part gjør gjeldende for å begrunne sin overbevisning om at målet for den elektroniske overvåkingen er en fremmed makt eller en agent for en fremmed makt, kan sistnevnte omfatte ikke-amerikanske personer involvert i internasjonal terrorisme eller internasjonal spredning av masseødeleggelsesvåpen (herunder forberedelser) (50 U.S.C. § 1801 (b) (1)). Det er imidlertid bare en teoretisk forbindelse til personopplysninger overført innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, ettersom det i redegjørelsen for de faktiske forholdene også må begrunnes at «hver av fasilitetene eller hvert sted som den elektroniske overvåkingen er rettet mot, anvendes, eller snart vil bli anvendt av en fremmed makt eller en agent for en fremmed makt». For å gjøre gjeldende dette rettslige grunnlaget skal det i alle tilfeller inngis en anmodning til FISC, som på grunnlag av de inngitte fakta blant annet vil vurdere om det finnes en rimelig grunn til at dette faktisk er tilfellet.

([81]) 50 U.S.C. § 1842 sammenholdt med § 1841 (2) og avsnitt 3127 i Title 18. Denne myndigheten gjelder ikke kommunikasjonens innhold, men derimot opplysninger om kunden eller abonnenten som bruker en tjeneste (f.eks. navn, adresse, abonnentnummer, den mottatte tjenestens lengde/type, betalingskilde/-metode). I denne forbindelse skal det inngis en anmodning om avgjørelse til FISC (eller til en amerikansk fredsdommer («magistrate judge»)) og brukes et spesifikt utvalgskriterium i henhold til § 1841 (4), dvs. et kriterium som spesifikt identifiserer en person, konto osv., og som i størst mulig grad brukes til å begrense mengden opplysninger som vil bli innhentet.

([82]) Selv om FBI i henhold til avsnitt 501 i FISA (tidligere avsnitt 215 i U.S. PATRIOT ACT) har myndighet til å anmode om en rettsavgjørelse for å få utlevert «håndgripelige ting» («tangible things») (særlig telefonmetadata, men også forretningsdokumenter) i forbindelse med utenlandsetterretning, kan enheter innen det amerikanske etterretningssamfunnet i henhold til avsnitt 702 i FISA søke om tilgang til opplysninger, herunder innhold i internettkommunikasjon, som kommer fra De forente stater, men der målet er visse ikke-amerikanske personer utenfor De forente stater.

([83]) På grunnlag av denne bestemmelsen kan FBI anmode om «håndgripelige ting» («tangible things») (f.eks. registre, papirer, dokumenter) ved å dokumentere overfor Foreign Intelligence Surveillance Court (FISC) at det er rimelige grunner til å tro at de er relevante for en spesifikk FBI-etterforskning. I sine søk må FBI bruke FISC-godkjente utvalgskriterier, og det skal finnes en «rimelig uttalt mistanke» om at et slikt kriterium er knyttet til en eller flere fremmede makter eller deres agenter som er involvert i internasjonal terrorisme eller forberedelse av dette. Se PCLOB, avsnitt 215 Report, s. 59, NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. januar 2016, s. 4–6.

([84]) ODNIs redegjørelser (vedlegg VI), s. 13 (note 38).

([85]) Se fotnote 81.

([86]) PCLOB, Sec. 702 Report, s. 32–33 med ytterligere henvisninger. Ifølge sitt personvernkontor skal NSA kontrollere at det er en forbindelse mellom målet og utvalgskriteriet samt dokumentere utenlandsetterretningen som antas å bli innhentet; disse opplysningene skal gjennomgås og godkjennes av to senioranalytikere i NSA, og hele prosessen vil bli sporet og senere gjennomgått av ODNI og det amerikanske justisdepartementet med tanke på om kravene overholdes. Se NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16. april 2014.

Oversight Board (PCLOB) er overvåking som utføres i henhold til avsnitt 702, dermed «utelukkende rettet mot spesifikke [ikke-amerikanske] personer som er blitt individuelt identifisert»([87]). Som følge av en «utløpsklausul» skal avsnitt 702 i FISA gjennomgås på nytt i 2017, og Kommisjonen skal på dette tidspunkt foreta en ny vurdering av de garantiene som er tilgjengelige for registrerte i EU.

82) I sine redegjørelser har den amerikanske regjering dessuten uttrykkelig forsikret Europakommisjonen om at det amerikanske etterretningssamfunnet «ikke driver vilkårlig overvåking av noen, herunder vanlige europeiske borgere»([88]). Når det gjelder personopplysninger innsamlet i De forente stater, støttes denne uttalelsen av empirisk dokumentasjon som viser at *anmodninger om innsyn* ved bruk av nasjonale sikkerhetsbrev (NSL) og i henhold til FISA, både hver for seg og sammen, bare gjelder et relativt lite antall mål sammenlignet med den samlede datastrømmen på internett([89]).

83) Når det gjelder *tilgang* til innsamlede opplysninger og *datasikkerhet*, krever PPD-28 at tilgang «skal begrenses til autorisert personell som har behov for opplysningene for å kunne utføre sine oppgaver», og at personopplysninger «skal behandles og lagres på en måte som sikrer et tilstrekkelig vern og hindrer at uautoriserte får tilgang, i samsvar med gjeldende garantier som gjelder for sensitive opplysninger». Etterretningspersonell får egnet og hensiktsmessig opplæring i prinsippene fastsatt i PPD-28([90]).

84) Når det gjelder *lagring* og videre *spredning* av personopplysninger fra registrerte i EU som er samlet inn av amerikanske etterretningsmyndigheter, angis det i PPD-28 at alle personer (herunder ikke-amerikanske personer) bør behandles med verdighet og respekt, at alle personer har berettigede personverninteresser når det gjelder behandlingen av deres personopplysninger, og at enheter innen etterretningssamfunnet derfor må innføre retningslinjer som gir tilstrekkelige garantier for denne typen opplysninger, og som i «rimelig grad er utformet for å minimere spredning og lagring av personopplysninger»([91]).

([87]) PLCOB, Sec. 702 Report, s. 111. Se også ODNIs redegjørelser (vedlegg VI), s. 9 («Innsamling i henhold til avsnitt 702 i [FISA] er ikke «massiv og vilkårlig», men er spesifikt rettet mot innsamling av utenlandsetterretning fra individuelt identifiserte berettigede mål») og s. 13, nr. 36 (med henvisning til en uttalelse fra FISC fra 2014), NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16. april 2014. Selv i forbindelse med UPSTREAM kan NSA bare anmode om oppfanging av elektronisk kommunikasjon til, fra eller om utvalgte utvalgskriterier.

([88]) ODNIs redegjørelser (vedlegg VI), s. 18. Se også s. 6 der det angis at gjeldende prosedyrer «viser at det er en klar vilje til å hindre vilkårlig innsamling av signaletterretningsinformasjon og – på høyeste regjeringsnivå – til å gjennomføre prinsippet om rimelighet.»

([89]) Se Statistical Transparency Report Regarding Use of National Security Authorities, 22. april 2015. Når det gjelder den generelle strømmen av opplysninger på internett, se f.eks. Fundamental Rights Agency, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), s. 15–16. Ifølge en nedgradert FISC-uttalelse fra 2011 kom over 90 % av den elektroniske kommunikasjonen innhentet i henhold til avsnitt 702 i FISA fra PRISM-programmet, mens mindre enn 10 % kom fra UPSTREAM. Se FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (tilgjengelig på http://www.dni.gov/files/documents /0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Se avsnitt 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 av 28. juli 2014, s. 5, der det anføres at «retningslinjene til enheter innen etterretningssamfunnet bør styrke eksisterende analysepraksis og -standarder med krav om at analytikere skal strukturere sine forespørsler eller andre søketermer og -teknikker for å identifisere etterretningsinformasjon som er relevant for en gyldig etterretnings- eller rettshåndhevingsoppgave, fokusere forespørsler om personer på kategorier av etterretningsinformasjon som oppfyller et etterretnings- eller rettshåndhevingskrav, og minimere gjennomgåelsen av personopplysninger som ikke er relevante i forbindelse med etterretnings- og rettshåndhevingskrav.» 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 enheter innen etterretningssamfunnet (herunder FBI, CIA og NSA) truffet tiltak med henblikk på å opplyse sitt personell om kravene i PPD-28 ved å utarbeide nye eller endre eksisterende retningslinjer for opplæring.

([91]) Ifølge ODNIs redegjørelser får disse begrensningene anvendelse uavhengig av om opplysningene ble masseinnsamlet eller innsamlet på en målrettet måte, og uavhengig av personens statsborgerskap.

85) Den amerikanske regjering har forklart at dette kravet om rimelighet betyr at enheter innen etterretningssamfunnet ikke trenger å vedta «teoretisk mulige tiltak», men «at innsatsen for å verne berettigede interesser knyttet til personvern og borgerlige frihetsrettigheter skal stå i forhold til signaletterretningsaktivitetenes praktiske behov»([92]). I denne forbindelse vil ikke-amerikanske personer bli behandlet på samme måte som amerikanske personer i henhold til prosedyrene som er godkjent av den amerikanske justisministeren (Attorney-General)([93]).

86) I henhold til disse reglene er lagring vanligvis begrenset til høyst fem år, med mindre det er særlig fastsatt ved lov eller uttrykkelig besluttet av direktøren for National Intelligence etter en grundig vurdering av personvernhensyn – idet det tas hensyn til synspunktene fra ODNIs Civil Liberties Protection Officer samt fra ansvarlige for personvern og borgerlige frihetsrettigheter («privacy and civil liberties officials») i etterretningsbyråene – at fortsatt lagring er i den nasjonale sikkerhets interesse([94]). Spredning er begrenset til tilfeller der opplysningene er relevante for det underliggende formålet med innsamlingen og dermed oppfyller et godkjent krav med hensyn til utenlandsetterretning og rettshåndheving([95]).

87) Ifølge garantiene gitt av den amerikanske regjering kan personopplysninger ikke spres utelukkende fordi den berørte personen ikke er amerikansk, og «signaletterretning om en utenlandsk persons rutinemessige aktiviteter vil ikke bli ansett som utenlandsetterretning som kan spres eller oppbevares permanent alene av denne årsak, med mindre dette på annen måte oppfyller et godkjent behov for utenlandsetterretning»([96]).

88) På bakgrunn av det ovenstående konkluderer Kommisjonen med at De forente stater har regler som sørger for at eventuelle inngrep for formål knyttet til nasjonal sikkerhet i de grunnleggende rettighetene til personer hvis personopplysninger overføres fra Unionen til De forente stater innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, begrenses til det som er strengt nødvendig for å nå det aktuelle berettigede målet.

89) Som analysen over viser, sikrer amerikansk rett at overvåkingstiltak bare vil bli brukt til å innhente utenlandsetterretningsinformasjon, noe som utgjør et berettiget politisk mål([97]), og at de vil være så målrettede som mulig. Særlig vil

([92]) Se ODNIs redegjørelser (vedlegg VI).

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

([94]) Avsnitt 4 (a) (i) i PPD-28, ODNIs redegjørelser (vedlegg VI), s. 7. Når det gjelder personopplysninger innsamlet i henhold til avsnitt 702 i FISA, fastslås det f.eks. i NSAs FISC-godkjente minimeringsprosedyrer at metadata og ikke-vurdert innhold for PRISM som en regel kan oppbevares i høyst fem år, mens UPSTREAM-data kan oppbevares i høyst to år. NSA overholder disse grensene for lagring gjennom en automatisert prosess som sørger for at innsamlede opplysninger slettes ved utgangen av den aktuelle lagringsperioden. Se NSA avsnitt 702 i FISA, Minimization Procedures, avsnitt 7 samt avsnitt 6 (a) (1), NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. april 2014. Lagring i henhold til avsnitt 501 i FISA (tidligere avsnitt 215 i U.S. PATRIOT ACT) er også begrenset til fem år, med mindre personopplysningene er en del av en behørig godkjent spredning av utenlandsetterretning eller det amerikanske justisdepartementet skriftlig informerer NSA om at opplysningene skal oppbevares i forbindelse med pågående eller ventede tvister. Se NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. januar 2016.

([95]) I henhold til avsnitt 501 i FISA (tidligere avsnitt 215 i U.S. PATRIOT ACT) kan spredning av personopplysninger bare skje i forbindelse med terrorbekjempelse eller som bevis på lovbrudd, og i henhold til avsnitt 702 i FISA bare dersom det foreligger et gyldig utenlandsetterretnings- eller rettshåndhevingsformål. Jf. NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. april 2014, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. januar 2016. Se også NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7. oktober 2014.

([96]) ODNIs redegjørelser (vedlegg VI), s. 7 (med henvisning til Intelligence Community Directive (ICD) 203).

([97]) Domstolen har fastslått at nasjonal sikkerhet utgjør et berettiget politisk mål. Se Schrems, nr. 88. Se også Digital Rights Ireland and Others, nr. 42–44 og 51 der Domstolen fant at kampen mot grov kriminalitet, særlig organisert kriminalitet og terrorisme, i stor grad kan være avhengig av bruk av moderne etterforskningsteknikker. I motsetning til strafferettslig etterforskning som vanligvis går ut på å fastslå ansvar og skyld for tidligere atferd retrospektivt, går etterretningsaktiviteter ofte ut på å forebygge trusler mot nasjonal sikkerhet før en skade har skjedd. Slik etterforskning må derfor ofte omfatte et bredere spekter av mulige aktører («mål») og et større geografisk område. Jf. ECtHR, Weber and Saravia v Germany, avgjørelse av 29. juni 2006, saksnr. 54934/00, nr. 105–118 (om såkalt strategisk overvåking).

masseinnsamling bare unntaksvis være tillatt dersom målrettet innsamling ikke er mulig, og dette vil være ledsaget av ekstra garantier for å minimere mengden opplysninger som samles inn, samt etterfølgende tilgang til disse (som må være målrettet og bare være tillatt for særlige formål).

90) Etter Kommisjonens vurdering er dette i samsvar med standarden som Domstolen har satt i *Schrems*-dommen, som innebærer at lovgivning som medfører inngrep i de grunnleggende rettighetene som garanteres ved artikkel 7 og 8 i pakten, skal innføre «minstegarantier»([98]) og «ikke er begrenset til det som er strengt nødvendig når den på generelt grunnlag tillater lagring av alle personopplysningene til alle personer hvis opplysninger er blitt overført fra Den europeiske union til De forente stater uten noen form for differensiering, begrensning eller unntak på grunnlag av målet som forfølges, og uten at det fastsettes et objektivt kriterium som gjør det mulig å avgrense offentlige myndigheters tilgang til opplysningene og etterfølgende bruk av dem, for formål som er spesifikke, strengt begrensede og som kan begrunne inngrepene som både tilgangen til nevnte opplysninger samt anvendelsen av disse innebærer»([99]). Det vil heller ikke være ubegrenset innsamling og lagring av opplysninger om alle personer uten noen begrensninger eller ubegrenset tilgang. I redegjørelsene framlagt for Kommisjonen, herunder forsikringen om at amerikanske signaletterretningsaktiviteter bare berører en brøkdel av den kommunikasjonen som skjer via internett, utelukkes det dessuten at det vil være tilgang «på generelt grunnlag»([100]) til innholdet i den elektroniske kommunikasjonen.

3.1.2. Effektivt rettslig vern

91) Kommisjonen har vurdert både de eksisterende mekanismene i De forente stater for tilsyn med amerikanske etterretningsmyndigheters inngrep i personopplysninger som overføres til De forente stater, og den individuelle klageadgangen som registrerte i EU har.

Tilsyn

92) Det amerikanske etterretningssamfunnet er underlagt forskjellige kontroll- og tilsynsmekanismer som faller inn under statsmaktens tre grener. Disse omfatter interne og eksterne organer innen den utøvende gren, et antall kongresskomiteer samt enheter med ansvar for å føre rettslig tilsyn, særlig med aktiviteter som utføres innenfor rammen av Foreign Intelligence Surveillance Act.

93) For det første er amerikanske myndigheters etterretningsaktiviteter underlagt et omfattende tilsyn fra den utøvende grens side.

94) I henhold til PPD-28 avsnitt 4 (a) iv) skal retningslinjene og prosedyrene til enhetene innen etterretningssamfunnet «omfatte egnede tiltak for å fremme tilsynet med gjennomføringen av garantier for vern av personopplysninger», og disse tiltakene bør omfatte regelmessig revisjon([101]).

([98]) Schrems, nr. 91, med ytterligere henvisninger.
([99]) Schrems, nr. 93.
([100]) Jf. Schrems, nr. 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 (Compliance), FBI, Presidential Policy Directive 28 Policies and Procedures, avsnitt III (A) (4), (B) (4), NSA, PPD-28 Section 4 Procedures, 12. januar 2015, avsnitt 8.1, 8.6 (c).

95) I denne forbindelse er det innført flere tilsynsnivåer, herunder ansvarlige for borgerlige frihetsrettigheter eller personvern («civil liberties or privacy officers»), generalinspektører («Inspector Generals»), ODNIs Civil Liberties and Privacy Office, PCLOB og President's Intelligence Oversight Board. Disse tilsynsfunksjonene støttes av personale med ansvar for spørsmål om overholdelse i alle byråene([102]).

96) Som forklart av den amerikanske regjering([103]) er det utpekt *ansvarlige for borgerlige frihetsrettigheter og personvern* med tilsynsansvar i forskjellige departementer med etterretningsansvar og i etterretningsbyråer([104]). Selv om den særlige myndigheten som disse tjenestemennene har, kan variere noe ut fra lovhjemmelen, omfatter den vanligvis tilsyn med prosedyrer for å sikre at det aktuelle departementet/byrået tar tilstrekkelig hensyn til personvernet og de borgerlige frihetsrettighetene og har innført egnede prosedyrer for å håndtere klager fra privatpersoner som mener at deres personvern eller borgerlige frihetsrettigheter er blitt krenket (og i noen tilfeller, f.eks. når det gjelder ODNI, har de selv myndighet til å undersøke klager([105])). Lederen for departementet/byrået skal sikre at nevnte tjenestemann mottar all informasjon og gis tilgang til alt materiale som vedkommende trenger for å kunne utføre sine funksjoner. De ansvarlige for borgerlige frihetsrettigheter og personvern rapporterer regelmessig til Kongressen og PCLOB, herunder om antall og typen klager som departementet/byrået har mottatt, og et sammendrag av utfallet av slike klager, gjennomgåelser og undersøkelser som er utført, samt konsekvensene av de aktivitetene som vedkommende har utført([106]). Ifølge vurderingen foretatt av de nasjonale personvernmyndighetene kan det interne tilsynet som utføres av slike ansvarlige, anses som «relativt robust», selv om de etter deres mening ikke i tilstrekkelig grad oppfyller kravet om uavhengighet([107]).

97) I tillegg har hver enhet innen etterretningssamfunnet sin egen *generalinspektør* («Inspector General») med ansvar for bl.a. å føre tilsyn med utenlandsetterretningsaktiviteter([108]). ODNI har f.eks. et eget generalinspektørkontor («Office of the Inspector General») med omfattende myndighet over hele etterretningssamfunnet og til å undersøke klager eller opplysninger om påstander om ulovlig praksis eller maktmisbruk i forbindelse med ODNIs og/eller etterretningssamfunnets programmer og aktiviteter([109]). Generalinspektører er enheter med lovfestet uavhengighet([110]) som har ansvar for å foreta revisjoner og undersøkelser i forbindelse med programmene og virksomheten som utføres av det aktuelle byrået for formål knyttet til nasjonal etterretning, herunder misbruk eller overtredelse av loven([111]). De har rett til å få tilgang til alle

([102]) NSA har f.eks. over 300 ansatte som arbeider med spørsmål om overholdelse i Directorate for Compliance. Se ODNIs redegjørelser (vedlegg VI), s. 7.

([103]) Se ombudsmekanismen (vedlegg III), avsnitt 6 bokstav b) i)–iii).

([104]) Se 42 U.S.C. § 2000ee-1. Dette omfatter f.eks. utenriksdepartementet (Department of State), justisdepartementet (Department of Justice) (herunder FBI), departementet for nasjonal sikkerhet (Department of Homeland Security), forsvarsdepartementet (Department of Defense), NSA, CIA og ODNI.

([105]) Ifølge den amerikanske regjering vil ODNIs Civil Liberties and Privacy Office, dersom kontoret mottar en klage, også samordne samarbeidet med andre enheter innen etterretningssamfunnet om hvordan klagen bør behandles videre i etterretningssamfunnet. Se ombudsmekanismen (vedlegg III), avsnitt 6 bokstav b) ii).

([106]) Se 42 U.S.C. § 2000ee-1 (f) (1), (2).

([107]) Artikkel 29-arbeidsgruppen for personvern, uttalelse 1/2016 om Privacy Shield-avtalen mellom EU og De forente stater – utkast til beslutning om tilstrekkelig beskyttelsesnivå (vedtatt 13. april 2016), s. 41.

([108]) ODNIs redegjørelser (vedlegg VI), s. 7. Se f.eks. NSA, PPD-28 Section 4 Procedures, 12. januar 2015, avsnitt 8.1, CIA, Signals Intelligence Activities, s. 7 (Responsibilities).

([109]) Denne generalinspektøren (en funksjon som ble opprettet i oktober 2010) utnevnes av presidenten med Senatets godkjenning og kan bare avsettes av presidenten, ikke av DNI.

([110]) Disse generalinspektørene er fast ansatte og kan bare avsettes av presidenten, som skal underrette Kongressen skriftlig om årsakene til en eventuell avsettelse. Dette betyr ikke nødvendigvis at de overhodet ikke er underlagt instrukser. I noen tilfeller kan lederen for departementet forby generalinspektøren å innlede, gjennomføre eller fullføre en revisjon eller etterforskning dersom dette anses som nødvendig for å beskytte viktige nasjonale (sikkerhets)interesser. Kongressen må imidlertid holdes orientert om utøvelsen av denne myndigheten, og kan på dette grunnlag holde den respektive lederen ansvarlig. Se f.eks. Inspector General Act fra 1978, § 8 (generalinspektør for forsvarsdepartementet), § 8E (generalinspektør for justisdepartementet), § 8G (d)(2) (A), (B) (generalinspektør for NSA), 50. U.S.C. § 403q (b) (generalinspektør for CIA), Intelligence Authorization Act For Fiscal Year 2010, avsnitt 405 (f) (generalinspektør for etterretningssamfunnet). Ifølge de nasjonale personvernmyndighetenes vurdering er det trolig at generalinspektørene «oppfyller kriteriet for organisatorisk uavhengighet som definert av CJEU og Den europeiske menneskerettighetsdomstol (ECtHR), i det minste fra det tidspunktet da den nye utnevnelsesprosessen gjelder for alle.» Se artikkel 29-arbeidsgruppen for personvern, uttalelse 1/2016 om Privacy Shield-avtalen mellom EU og De forente stater – utkast til beslutning om tilstrekkelig beskyttelsesnivå (vedtatt 13. april 2016), s. 40.

([111]) Se ODNIs redegjørelser (vedlegg VI), s. 7. Se også Inspector General Act fra 1978 med etterfølgende endringer, Pub. L. 113-126 av 7. juli 2014.

registre, rapporter, revisjoner, gjennomgåelser, dokumenter, papirer, anbefalinger eller annet relevant materiale, ved behov på grunnlag av et pålegg («subpoena»), og kan innhente vitneutsagn([112]). Selv om generalinspektørene bare kan utstede ikke-bindende anbefalinger om korrigerende tiltak, offentliggjøres deres rapporter, herunder om oppfølgingstiltak (eller mangel på dette), og sendes til Kongressen som på dette grunnlag kan utøve sin tilsynsfunksjon([113]).

98) Dessuten har *Privacy and Civil Liberties Oversight Board* (PCLOB), som er et uavhengig organ([114]) innen den utøvende gren bestående av et styre([115]) på fem medlemmer fra de to største partiene som utnevnes av presidenten med Senatets godkjenning for en fast seksårsperiode, en rekke ansvarsområder knyttet til terrorbekjempelsespolitikk og gjennomføringen av dette med henblikk på å ivareta personvernet og de borgerlige frihetsrettighetene. Organet kan i forbindelse med sin gjennomgåelse av etterretningssamfunnets virksomhet få tilgang til alle relevante registre, rapporter, revisjoner, gjennomgåelser, dokumenter, papirer og anbefalinger, herunder gradert informasjon, og foreta intervjuer og innhente vitneutsagn. Det mottar rapporter fra ansvarlige for borgerlige frihetsrettigheter og personvern i en rekke føderale organer/byråer([116]), kan utstede anbefalinger til dem og rapporterer regelmessig til kongresskomiteer og presidenten([117]). PCLOB har, innenfor rammen av sitt mandat, også som oppgave å utarbeide en rapport med en vurdering av gjennomføringen av PPD-28.

99) De ovennevnte tilsynsmekanismene suppleres dessuten av *Intelligence Oversight Board* som er opprettet innenfor rammen av presidentens Intelligence Advisory Board, og som fører tilsyn med de amerikanske etterretningsmyndighetenes overholdelse av grunnloven og alle gjeldende regler.

100) For å lette tilsynet oppmuntres enheter innen etterretningssamfunnet til å utvikle informasjonssystemer som gjør det mulig å overvåke, registrere og gjennomgå forespørsler om eller andre søk etter personopplysninger([118]). Tilsyns- og kontrollorganer vil jevnlig kontrollere praksisen som enheter innen etterretningssamfunnet bruker for å verne personopplysninger som forekommer i signaletterretning, og at de overholder disse prosedyrene([119]).

101) Disse tilsynsfunksjonene støttes også av omfattende krav til rapportering av manglende overholdelse. Byråenes prosedyrer skal særlig sikre at alvorlige tilfeller av manglende overholdelse som omfatter personopplysningene til en hvilken som helst person, uavhengig av vedkommendes statsborgerskap, og som er samlet inn gjennom signaletterretning, omgående rapporteres til lederen for etterretningsenheten, som deretter vil underrette direktøren for National Intelligence, som i henhold til PPD-28 skal bestemme om det skal treffes korrigerende tiltak([120]). I henhold til E.O. 12333 skal dessuten alle enheter innen etterretningssamfunnet rapportere tilfeller av manglende overholdelse til Intelligence Oversight Board([121]). Disse mekanismene sikrer at problemet vil bli behandlet på høyeste hold i

([112]) Se Inspector General Act fra 1978, § 6.

([113]) Se ODNIs redegjørelser (vedlegg VI), s. 7. Se også Inspector General Act fra 1978, §§ 4(5), 5. I henhold til avsnitt 405 b) 3), 4) i Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 av 7. oktober 2010 skal generalinspektøren for etterretningssamfunnet holde DNI og Kongressen orientert om nødvendigheten av og status for korrigerende tiltak.

([114]) Ifølge de nasjonale personvernmyndighetenes vurdering har PCLOB tidligere vist sin uavhengighet. Se artikkel 29-arbeidsgruppen for personvern, uttalelse 1/2016 om Privacy Shield-avtalen mellom EU og De forente stater – utkast til beslutning om tilstrekkelig beskyttelsesnivå (vedtatt 13. april 2016), s. 42.

([115]) PCLOB har i tillegg rundt 20 fast ansatte. Se https://www.pclob.gov/about-us/staff.html.

([116]) Disse omfatter minst det amerikanske justisdepartement (Department of Justice), forsvarsdepartement (Department of Defense), departementet for nasjonal sikkerhet (Department of Homeland Security), direktøren for National Intelligence og Central Intelligence Agency samt andre departementer, byråer eller enheter innen den utøvende gren som PCLOB mener bør omfattes.

([117]) Se 42 U.S.C. § 2000ee. Se også ombudsmekanismen (vedlegg III), avsnitt 6 bokstav b) iv). PCLOB plikter bl.a. å rapportere når et byrå under den utøvende gren nekter å følge PCLOBs 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. 7-8.

([119]) Id. på s. 8. Se også ODNIs redegjørelser (vedlegg 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 Section 4 Procedures, 12. januar 2015, avsnitt 7.3, 8.7 (c), (d), FBI, Presidential Policy Directive 28 Policies and Procedures, avsnitt III. (A) (4), (B) (4), CIA, Signals Intelligence Activities, s. 6 (Compliance) og s. 8 (Responsibilities).

([121]) Se E.O. 12333, avsnitt 1.6 (c).

etterretningssamfunnet. Dersom en ikke-amerikansk person er involvert, skal direktøren for National Intelligence i samråd med utenriksministeren og lederen for melderorganet eller -byrået bestemme hvilke tiltak som skal treffes for å underrette den relevante utenlandske regjeringen, idet det tas hensyn til vern av kilder og metoder samt amerikansk personell([122]).

102) I tillegg til disse tilsynsmekanismene innen den utøvende gren har De forente staters kongress, særlig *Representantens hus' og Senatets etterretnings- og rettskomiteer*, tilsynsansvar med hensyn til alle amerikanske utenlandsetterretningsaktiviteter, herunder amerikansk signaletterretning. I henhold til National Security Act skal «presidenten sikre at Kongressens etterretningskomiteer orienteres fullt ut og løpende om De forente staters etterretningsaktiviteter, herunder om eventuelle omfattende planlagte etterretningsaktiviteter i henhold til det som kreves i dette underkapittel»([123]). I tillegg «skal presidenten sikre at eventuelle ulovlige etterretningsaktiviteter og ethvert korrigerende tiltak som er truffet eller planlagt i forbindelse med en slik ulovlig aktivitet, rapporteres omgående til Kongressens etterretningskomiteer»([124]). Medlemmene av disse komiteene har tilgang til gradert informasjon samt etterretningsmetoder og –programmer([125]).

103) I senere lover er rapporteringskravene blitt utvidet og presisert, både for enhetene innen etterretningssamfunnet, de relevante generalinspektørene og den amerikanske justisministeren. I henhold til FISA skal den amerikanske justisministeren (Attorney General) f.eks. «fullt ut informere» Representantenes hus' og Senatets etterretnings- og rettskomiteer om regjeringens aktiviteter i henhold til visse avsnitt i FISA([126]). Det stilles også krav om at regjeringen skal legge fram kopier av alle avgjørelser, kjennelser eller uttalelser fra Foreign Intelligence Surveillance Court eller Foreign Intelligence Surveillance Court of Review som inneholder en vesentlig forklaring eller fortolkning av FISA-bestemmelser, for kongresskomiteene. Med hensyn til overvåking i henhold til avsnitt 702 i FISA utøves tilsyn særlig gjennom lovfestede rapporter til etterretnings- og rettskomiteene og ved bruk av hyppige gjennomgåelser og høringer. Dette omfatter en halvårsrapport utarbeidet av den amerikanske justisministeren om anvendelsen av avsnitt 702 i FISA med underlagsdokumenter, herunder særlig justisdepartementets og ODNIs rapporter om overholdelse og en beskrivelse av eventuelle tilfeller av manglende overholdelse([127]), samt en separat halvårsvurdering utarbeidet av justisministeren og DNI som dokumenterer at målrettings- og minimeringsprosedyrene er overholdt, herunder prosedyrene som skal sikre at opplysninger samles inn for et gyldig utenlandsetterretningsformål([128]). Kongressen mottar også rapporter fra generalinspektørene som har myndighet til å vurdere i hvilken grad byråene overholder målrettings- og minimeringsprosedyrene og den amerikanske justisministerens generelle retningslinjer.

104) I henhold til USA FREEDOM Act fra 2015 skal den amerikanske regjering hvert år opplyse Kommisjonen (og allmennheten) om bl.a. antall FISA-kjennelser og -direktiver som det er anmodet om, og som er oppnådd, samt om anslått antall overvåkede amerikanske og ikke-amerikanske personer([129]). I loven stilles det også krav om offentliggjøring av

([122]) PPD-28, avsnitt 4 (a) (iv).

([123]) Se avsnitt 501 (a) (1) (50 U.S.C. § 413 (a) (1)). Denne bestemmelsen inneholder de generelle kravene med hensyn til Kongressens tilsyn på området nasjonal sikkerhet.

([124]) Se avsnitt 501 (b) (50 U.S.C. § 413 (b)).

([125]) Jf. avsnitt 501 (d) (50 U.S.C. § 413 (d)).

([126]) Se 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

([127]) Se 50 U.S.C. § 1881f.

([128]) Se 50 U.S.C. § 1881a (l) (1).

([129]) Se USA FREEDOM Act fra 2015, Pub. L. No 114-23, avsnitt 602 (a). I henhold til avsnitt 402 skal «direktøren for National Intelligence i samråd med den amerikanske justisministeren foreta en vurdering med tanke på nedgradering av hver avgjørelse, kjennelse eller uttalelse utstedt av Foreign Intelligence Surveillance Court eller Foreign Intelligence Surveillance Court of Review (som definert i avsnitt 601 (e)) som inneholder en vesentlig fortolkning eller forklaring av innholdet i eller hensikten med en lovbestemmelse, herunder en ny eller vesentlig fortolkning eller forklaring av termen «spesifikt utvalgskriterium» («specific selection term»), og, i samsvar med nevnte gjennomgåelse, i størst mulig grad gjøre slike avgjørelser, kjennelser eller uttalelser offentlig tilgjengelige.»

antall utstedte nasjonale sikkerhetsbrev (NSL), også dette vedrørende amerikanske og ikke-amerikanske personer (samtidig som mottakere av FISA-kjennelser og -sertifiseringer samt NSL-anmodninger får mulighet til å utstede innsynsrapporter på visse vilkår)([130]).

105) Etterretningsaktiviteter som utføres av amerikanske offentlige myndigheter basert på FISA, er underlagt *FISA-domstolens* (FISC)([131]) prøvingsrett, og tiltakene skal i noen tilfeller forhåndsgodkjennes av nevnte domstol, som er en uavhengig domstol([132]), hvis avgjørelser kan bringes inn for Foreign Intelligence Court of Review (FISCR)([133]) og i siste instans for De forente staters høyesterett([134]). Når det gjelder forhåndsgodkjenning, skal anmodende myndigheter (FBI, NSA, CIA osv.) sende et utkast til anmodning til advokater i justisdepartementets National Security Department som vil gjennomgå det og eventuelt be om ytterligere informasjon([135]). Når anmodningen er utarbeidet, skal den godkjennes av justisministeren (Attorney General), visejustisministeren (Deputy Attorney General) eller assisterende minister for nasjonal sikkerhet (Assistant Attorney General for National Security)([136]). Justisdepartementet vil deretter sende anmodningen til FISC, som vil vurdere den og treffe en foreløpig avgjørelse om det videre forløpet([137]). Dersom det arrangeres en høring, har FISC myndighet til å innhente vitneutsagn og råd fra sakkyndige([138]).

106) FISC (og FISCR) støttes av et fast panel bestående av fem privatpersoner med ekspertise innen nasjonal sikkerhet og borgerlige frihetsrettigheter([139]). Fra denne gruppen skal domstolen utnevne en person som skal fungere som *amicus curiae* og bistå i vurderingen av anmodninger om kjennelse eller prøving som etter domstolens mening utgjør en ny eller vesentlig fortolkning av loven, med mindre domstolen finner at en slik utnevnelse ikke er hensiktsmessig([140]). Dette skal særlig sikre at hensynet til personvern avspeiles behørig i domstolens vurdering. Domstolen kan også utnevne en person eller organisasjon som skal fungere som *amicus curiae*, herunder bistå med teknisk ekspertise, når den anser dette som hensiktsmessig, eller, på anmodning, tillate en person eller organisasjon å inngi en *amicus curiae*-rapport([141]).

([130]) USA FREEDOM Act, avsnitt 602 (a), 603 (a).

([131]) For visse typer overvåking kan en amerikansk fredsdommer («magistrate judge») som er offentlig oppnevnt av De forente staters høyesterettsjustitiarius (Chief Justice), ha myndighet til å behandle anmodninger og avsi kjennelser.

([132]) FISC består av elleve dommere som er utnevnt av De forente staters høyesterettsjustitiarius (Chief Justice) blant sittende dommere ved amerikanske distriktsdomstoler utnevnt av presidenten og godkjent av Senatet. Dommerne er ansatt på livstid og kan bare avsettes med god grunn. De tjenestegjør ved FISC i 7-årsperioder og skiftes ikke ut samtidig. FISA krever at dommerne hentes fra minst sju forskjellige amerikanske rettskretser. Se avsnitt 103 i FISA (50 U.S.C. 1803 (a)), PCLOB, Sec. 215 Report, s. 174–187. Dommerne bistås av erfarne dommerfullmektiger som utgjør domstolens juridiske personell, og som utarbeider juridiske analyser av anmodninger om innsamling. Se PCLOB, avsnitt 215 Report, s. 178, brev fra Reggie B. Walton, rettsformann for U.S. Foreign Intelligence Surveillance Court, til Patrick J. Leahy, formann for Committee on the Judiciary, U.S. Senate (29. juli 2013) («Walton-brevet»), s. 2–3.

([133]) FISCR består av tre dommere som er utpekt av De forente staters høyesterettsjustitiarius (Chief Justice), og som hentes fra amerikanske distriktsdomstoler eller ankedomstoler. De sitter i 7-årsperioder og skiftes ikke ut samtidig. Se avsnitt 103 i FISA (50 U.S.C. § 1803 (b)).

([134]) Se 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i) (4).

([135]) For eksempel ytterligere saksinformasjon om målet for overvåkingen, teknisk informasjon om overvåkingsmetoden eller garantier om hvordan opplysningene som samles inn, vil bli brukt og spredd. Se PCLOB, avsnitt 215 Report, s. 177.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) FISC kan godkjenne anmodningen, be om ytterligere informasjon, beslutte om det er nødvendig å gjennomføre en høring eller eventuelt avslå anmodningen. Regjeringen vil utarbeide sin endelige anmodning på bakgrunn av denne foreløpige avgjørelsen. På bakgrunn av dommerens innledende kommentarer kan anmodningen inneholde vesentlige endringer i forhold til den opprinnelige anmodningen. Selv om FISC godkjenner en stor prosentandel av de endelige anmodningene, inneholder en betydelig del av disse vesentlige endringer i forhold til den opprinnelige anmodningen, f.eks. 24 % av anmodningene som ble godkjent i perioden fra juli til september 2013. Se PCLOB, avsnitt 215 Report, s. 179, Walton-brevet, s. 3.

([138]) PCLOB, avsnitt 215 Report, s. 179, note 619.

([139]) 50 U.S.C. § 1803 (i) (1), (3) (A). Denne nye lovgivningen gjennomførte PCLOBs anbefalinger om å opprette en gruppe av eksperter på personvern og borgerlige frihetsrettigheter som kan fungere som amicus curiae, med det formål å gi domstolen juridiske argumenter med hensyn til fremming av personvern og borgerlige frihetsrettigheter. Se PCLOB, avsnitt 215 Report, s. 183–187.

([140]) 50 U.S.C. § 1803 (i) (2) (A). Ifølge informasjon fra ODNI har slike utnevnelser allerede skjedd. Se Signals Intelligence Reform, 2016 Progress Report.

([141]) 50 U.S.C. § 1803 (i) (2) (B).

107) Når det gjelder de to rettslige godkjenningene til å foreta overvåking i henhold til FISA, og som er viktigst med hensyn til dataoverføringer innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, varierer FISCs tilsyn.

108) I henhold til avsnitt 501 i FISA([142]), som tillater innsamling av «håndgripelige ting» («tangible things») (herunder bøker, registre, papirer, dokumenter og andre elementer), skal anmodningen til FISC inneholde en redegjørelse for sakens fakta som viser at det er rimelige grunner til å tro at de håndgripelige tingene som ønskes innsamlet, er relevante for en godkjent undersøkelse (unntatt trusselvurderinger) som utføres for å innhente utenlandsetterretningsinformasjon om ikke-amerikanske personer, eller beskytte mot internasjonal terrorisme eller hemmelige etterretningsaktiviteter. Anmodningen skal også inneholde en liste over minimeringsprosedyrene som den amerikanske justisministeren har innført med henblikk på oppbevaring og spredning av den innsamlede etterretningen([143]).

109) I henhold til avsnitt 702 i FISA([144]) tillater FISC derimot ikke individuelle overvåkingstiltak, men isteden overvåkingsprogrammer (f.eks. PRISM, UPSTREAM) på grunnlag av årlige sertifiseringer utarbeidet av den amerikanske justisministeren og direktøren for National Intelligence. I henhold til avsnitt 702 i FISA tillates målrettet overvåking av personer som det er rimelig grunn til å tro befinner seg utenfor De forente stater, med henblikk på innhenting av utenlandsetterretningsinformasjon([145]). Slik målretting utføres av NSA i to trinn: Først foretar NSAs analytikere en identifisering av ikke-amerikanske personer som befinner seg i utlandet, og der overvåking ifølge analytikerne vil føre til innhenting av den relevante utenlandsetterretningen som er angitt i sertifiseringen. Når disse privatpersonene er identifisert og målrettet overvåking av disse er godkjent på grunnlag av en grundig vurderingsmekanisme i NSA([146]), vil utvalgskriterier som identifiserer kommunikasjonselementer (f.eks. e-postadresser), som målene bruker, bli utvalgt (dvs. utarbeidet og brukt)([147]). Som angitt inneholder sertifiseringene som skal godkjennes av FISC, ingen informasjon om de enkelte personene som det skal foretas målrettet overvåking av, men de identifiserer isteden kategorier av utenlandsetterretningsinformasjon([148]). Selv om FISC – på bakgrunn av en rimelig grunn eller andre kriterier – ikke foretar en vurdering av om målrettingen av privatpersoner er velegnet med tanke på innsamling av utenlandsetterretningsinformasjon([149]), kan opplysninger likevel samles inn på det vilkår at «et vesentlig formål med innsamlingen er å innhente utenlandsetterretningsinformasjon»([150]). I henhold til avsnitt 702 i FISA kan NSA samle inn kommunikasjon fra ikke-amerikanske personer utenfor De forente stater bare dersom det er rimelig grunn til å tro at et gitt kommunikasjonsmiddel brukes til å kommunisere utenlandsetterretningsinformasjon (f.eks. knyttet til internasjonal terrorisme, kjernefysisk spredning eller fiendtlige internettaktiviteter). Slike avgjørelser er underlagt domstolskontroll([151]). Sertifiseringene skal også inneholde målrettings- og minimeringsprosedyrer([152]). Den amerikanske justisministeren og

([142]) 50 U.S.C. § 1861
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) PCLOB, avsnitt 702 Report, s. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). Ifølge PCLOB har disse kategoriene så langt hovedsakelig omfattet internasjonal terrorisme og spørsmål som f.eks. erverv av masseødeleggelsesvåpen. Se PCLOB, avsnitt 702 Report, s. 25.
([149]) PCLOB, avsnitt 702 Report, s. 27.
([150]) 50 U.S.C. § 1881a.
([151]) «Liberty and Security in a Changing World», rapport og anbefalinger fra President's Review Group on Intelligence and Communications Technologies, 12. desember 2013, s. 152.
([152]) 50 U.S.C.1881a (i).

direktøren for National Intelligence kontrollerer overholdelsen, og byråene plikter å rapportere om eventuelle tilfeller av manglende overholdelse til FISC([153]) (samt Kongressen og President's Intelligence Oversight Board), som på dette grunnlaget kan endre godkjenningen([154]).

110) For å gjøre FISCs tilsyn mer effektivt har De forente staters administrasjon dessuten samtykket i å gjennomføre en anbefaling fra PCLOB om å legge fram dokumentasjon for FISC om avgjørelser om målrettet overvåking som er truffet i henhold til avsnitt 702, herunder et vilkårlig utvalg av skjemaer over overvåkingsmål, slik at FISC kan vurdere hvordan kravet om utenlandsetterretningsformål oppfylles i praksis([155]). Samtidig har administrasjonen i De forente stater akseptert og truffet tiltak for å revidere NSAs målrettingsprosedyrer for bedre å dokumentere utenlandsetterretningsformålene som ligger til grunn for avgjørelser om målrettet overvåking([156]).

Individuell klageadgang

111) I henhold til amerikansk rett har registrerte i EU en rekke muligheter dersom de lurer på om deres personopplysninger er blitt behandlet (innsamlet, vurdert osv.) av enheter innen det amerikanske etterretningssamfunnet, og, dersom dette er tilfellet, om gjeldende begrensninger i amerikansk rett er blitt overholdt. Dette gjelder særlig tre områder: Inngrep i henhold til FISA, statstjenestemenns ulovlige og bevisste tilgang til personopplysninger samt innsyn i opplysninger i henhold til Freedom of Information Act (FOIA)([157]).

112) For det første inneholder Foreign Intelligence Surveillance Act en rekke rettsmidler som også er tilgjengelige for ikke-amerikanske personer, og som kan brukes til å klage på ulovlig elektronisk overvåking([158]). Dette omfatter privatpersoners mulighet til å anlegge sivilt søksmål om økonomisk erstatning mot De forente stater dersom opplysninger om vedkommende er blitt ulovlig og bevisst brukt eller utlevert([159]), til å saksøke statstjenestemenn i De forente stater personlig («i lovens navn») for å oppnå økonomisk erstatning([160]) og til å bestride lovligheten av overvåkingen (og anmode om å få opplysningene fjernet) dersom den amerikanske regjering akter å bruke eller utlevere opplysninger som er innhentet ved eller utledet av elektronisk overvåking, mot privatpersonen i rettslige eller administrative prosedyrer i De forente stater([161]).

113) For det andre har den amerikanske regjering informert Kommisjonen om en rekke andre muligheter som registrerte i EU kan benytte seg av for å anlegge sak mot statstjenestemenn for ulovlig tilgang til eller bruk av personopplysninger,

([153]) I henhold til regel 13 (b) i FISCs forretningsorden skal regjeringen umiddelbart underrette domstolen skriftlig dersom den oppdager at en myndighet eller tillatelse gitt av domstolen er blitt gjennomført på en måte som ikke er i samsvar med domstolens godkjenning eller tillatelse eller med gjeldende rett. Den krever også at regjeringen skal underrette domstolen skriftlig om de faktiske forholdene og omstendighetene som er relevante for den manglende overholdelsen. Regjeringen vil vanligvis avgi en skriftlig underretning i henhold til regel 13 (a) når de relevante faktiske forholdene er kjente, og når enhver uautorisert innsamling er blitt destruert. Se Walton-brevet, s. 10.

([154]) 50 U.S.C. § 1881 (l). Se også PCLOB, avsnitt 702 Report, s. 66–76, NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. april 2014. Innsamling av personopplysninger for etterretningsformål i henhold til avsnitt 702 i FISA er underlagt både internt og eksternt tilsyn fra den utøvende grens side. Det interne tilsynet omfatter bl.a. interne programmer for å vurdere og føre tilsyn med overholdelsen av målrettings- og minimeringsprosedyrer, rapportering av tilfeller av manglende overholdelse både internt og eksternt til ODNI, det amerikanske justisdepartementet, Kongressen og FISC og årlige gjennomgåelser som sendes til disse organene. Når det gjelder eksternt tilsyn, består det hovedsakelig av målrettings- og minimeringsvurderinger som utføres av ODNI, justisdepartementet og generalinspektører, og som rapporterer til Kongressen og FISC, herunder om tilfeller av manglende overholdelse. Alvorlige tilfeller av manglende overholdelse må rapporteres til FISC umiddelbart, mens andre rapporteres i kvartalsrapporter. Se PCLOB, avsnitt 702 Report, s. 66-77.

([155]) PCLOB, Recommendations Assessment Report, 29. januar 2015, s. 20.

([156]) PCLOB, Recommendations Assessment Report, 29. januar 2015, s. 16.

([157]) I avsnitt 10 i Classified Information Procedures Act er det dessuten fastsatt at i ethvert søksmål der det kreves at De forente stater dokumenterer at et materiale er gradert (f.eks. fordi det må beskyttes mot uautorisert utlevering av hensyn knyttet til nasjonal sikkerhet), skal De forente stater underrette den saksøkte om hvilke deler av materialet som med rimelighet forventes å bli brukt for å dokumentere at et element knyttet til lovovertredelsen er gradert.

([158]) Se ODNIs redegjørelser (vedlegg VI), s. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

herunder for påståtte formål knyttet til nasjonal sikkerhet (dvs. Computer Fraud and Abuse Act([162]), Electronic Communications Privacy Act([163]) og Right to Financial Privacy Act([164])). Alle disse søksmålsgrunnlagene gjelder spesifikke opplysninger, mål og/eller typer tilgang (f.eks. fjerntilgang til en datamaskin via internett) og er tilgjengelige på visse vilkår (f.eks. bevisste handlinger, handlinger som ikke utføres innenfor rammen av et offisielt verv, lidd skade)([165]). En mer generell klagemulighet finnes i Administrative Procedure Act (5 U.S.C. § 702), der det angis at «enhver person som lider rettslig urett som følge av et byrås handlinger, eller som er blitt krenket eller forurettet av et byrås handlinger», har rett til å anmode om domstolskontroll. Dette omfatter muligheten til å be domstolen om å «erklære ulovlig og sette til side et byrås tiltak, funn og konklusjoner som anses for å være […] vilkårlige, ustadige eller et uttrykk for maktmisbruk, eller som på annen måte ikke er i samsvar med loven»([166]).

114) Den amerikanske regjering har dessuten pekt på at ikke-amerikanske personer kan bruke FOIA som grunnlag for å søke om innsyn i eksisterende føderale byråers registre, herunder dersom de inneholder vedkommendes personopplysninger([167]). Med tanke på FOIAs virkeområde gir loven ikke en privatperson mulighet til å motsette seg inngrep i personopplysninger som sådan, selv om den i prinsippet kan gjøre det mulig for privatpersoner å få innsyn i relevante opplysninger som innehas av nasjonale etterretningsbyråer. Selv på dette området er mulighetene tilsynelatende begrenset, ettersom byråer kan holde tilbake opplysninger som omfattes av visse angitte unntak, herunder innsyn i gradert informasjon knyttet til nasjonal sikkerhet og informasjon som gjelder etterforskning i forbindelse med rettshåndheving([168]). Når dette er sagt, kan nasjonale etterretningsbyråers bruk av slike unntak bestrides av privatpersoner, som kan anmode om både administrativ og rettslig prøving.

115) Selv om privatpersoner, herunder registrerte i EU, derfor har en rekke klagemuligheter når de har vært gjenstand for ulovlig (elektronisk) overvåking for formål knyttet til nasjonal sikkerhet, er det også klart at i hvert fall noe av det rettslige grunnlaget som amerikanske etterretningsmyndigheter kan bruke (f.eks. E.O. 12333), ikke omfattes. Selv om ikke-amerikanske privatpersoner i prinsippet har mulighet til å be om rettslig prøving, f.eks. i forbindelse med overvåking i henhold til FISA, er tilgjengelige søksmålsgrunnlag begrensede([169]), og søksmål fra privatpersoner (herunder amerikanske) vil bli avvist dersom de ikke kan dokumentere sin søksmålskompetanse([170]), noe som gir begrenset adgang til alminnelige domstoler([171]).

116) For å gi alle registrerte i EU nok et rettsmiddel har den amerikanske regjering besluttet å opprette en ny ombudsmekanisme, som omhandlet i brevet fra De forente staters utenriksminister til Kommisjonen i vedlegg III til denne beslutning. Denne mekanismen er basert på at det i henhold til PPD-28 utpekes en seniorkoordinator (på statssekretærnivå) i det amerikanske utenriksdepartementet som skal fungere som kontaktpunkt for utenlandske regjeringer ved spørsmål angående amerikanske signaletterretningsaktiviteter, men som går betydelig lenger enn dette opprinnelige konseptet.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701–2712.
([164]) 12 U.S.C. § 3417.
([165]) ODNIs redegjørelser (vedlegg VI), s. 17.
([166]) 5 U.S.C. § 706 (2) (A).
([167]) 5 U.S.C. § 552. Det finnes lignende lover på delstatsplan.
([168]) I dette tilfellet vil vedkommende vanligvis bare motta et standardsvar der byrået avslår enten å bekrefte eller avkrefte at det foreligger slike registre. Se ACLU v CIA, 710 F.3d 422 (D.C. Cir. 2014).
([169]) Se ODNIs redegjørelser (vedlegg VI), s. 16. Ifølge de framlagte forklaringene er tilgjengelige søksmålsgrunnlag enten at det foreligger skade (18 U.S.C. § 2712, 50 U.S.C. § 1810) eller dokumentasjon på at regjeringen akter å bruke eller utlevere opplysninger innhentet ved eller utledet av elektronisk overvåking av den berørte personen mot den berørte personen i forbindelse med rettslige eller administrative prosedyrer i De forente stater (50 U.S.C. § 1806). Domstolen har imidlertid flere ganger understreket at for å fastslå om det foreligger et inngrep i den grunnleggende retten til privatliv, har det ingen betydning om inngrepet har medført eventuelle ubehageligheter for den berørte. Se Schrems, nr. 89, med ytterligere henvisninger.
([170]) Dette godtakbarhetskriteriet er basert på kravet om sak eller tvistemål («case or controversy») i artikkel III i den amerikanske grunnloven.
([171]) Se Clapper v Amnesty Int'l USA, 133 S.Ct. 1138, 1144 (2013). Når det gjelder bruk av nasjonale sikkerhetsbrev (NSL), er det i USA FREEDOM Act (avsnitt 502 (f)–503) fastsatt at krav om hemmelighold må gjennomgås regelmessig, og at mottakere av NSL skal underrettes når de faktiske forholdene ikke lenger støtter et krav om hemmelighold (se ODNIs redegjørelser (vedlegg VI), s. 13). Dette sikrer imidlertid ikke at den registrerte i EU underrettes om at vedkommende har vært gjenstand for en undersøkelse.

117) Ifølge de forpliktende tilsagnene fra den amerikanske regjering vil ombudsmekanismen sikre at individuelle klager blir korrekt undersøkt og behandlet, og at privatpersoner mottar en uavhengig bekreftelse på at amerikansk rett er blitt overholdt, eller, ved en eventuell manglende overholdelse av lovgivningen, at dette er blitt rettet opp([172]). Mekanismen omfatter «Privacy Shield-ombudet», dvs. statssekretæren og annet personell samt andre tilsynsorganer med kompetanse til å føre tilsyn med de forskjellige enhetene innen etterretningssamfunnet som Privacy Shield-ombudet skal samarbeide med i behandlingen av klager. Særlig i tilfeller der en privatpersons anmodning gjelder hvorvidt overvåkingen er forenlig med amerikansk rett, vil Privacy Shield-ombudet kunne støtte seg på uavhengige tilsynsorganer med undersøkelsesmyndighet (f.eks. generalinspektørene eller PCLOB). I hvert tilfelle skal den amerikanske utenriksministeren sikre at ombudet har nødvendige midler for å sikre at svar på individuelle anmodninger bygger på all nødvendig informasjon.

118) Gjennom denne «sammensatte strukturen» garanterer ombudsmekanismen uavhengig tilsyn og individuell klageadgang. Samarbeidet med andre tilsynsorganer sikrer også tilgang til nødvendig ekspertise. Ved å pålegge Privacy Shield-ombudet å bekrefte overholdelse eller rette opp en eventuell manglende overholdelse, gjenspeiler mekanismen den amerikanske regjeringens generelle plikt til å behandle og avgjøre klager fra privatpersoner i EU.

119) For det første vil Privacy Shield-ombudet, til forskjell fra en ren mellomstatlig mekanisme, motta og svare på individuelle klager. Slike klager kan rettes til tilsynsmyndighetene i medlemsstatene med kompetanse til å føre tilsyn med nasjonale sikkerhetstjenester og/eller offentlige myndigheters behandling av personopplysninger, som vil videresende dem til et sentralisert EU-organ, som vil kanalisere dem til Privacy Shield-ombudet([173]). Dette vil faktisk være en fordel for privatpersoner i EU som dermed kan henvende seg til en nasjonal myndighet i nærheten og på sitt eget språk. Denne myndigheten skal bistå personen med å utarbeide en anmodning som inneholder grunnleggende informasjon og kan regnes som «fullstendig», til Privacy Shield-ombudet. Personen trenger ikke å dokumentere at den amerikanske regjering rent faktisk har fått tilgang til vedkommendes personopplysninger gjennom signaletterretningsaktiviteter.

120) For det andre forplikter den amerikanske regjering seg til å sikre at Privacy Shield-ombudet, i utførelsen av sine funksjoner, kan samarbeide med andre mekanismer for tilsyn med og kontroll av overholdelse som foreligger i amerikansk rett. Dette vil noen ganger omfatte nasjonale etterretningsmyndigheter, særlig dersom en anmodning kan tolkes som en anmodning om innsyn i dokumenter i henhold til Freedom of Information Act. I andre tilfeller, særlig dersom anmodninger gjelder hvorvidt overvåkingen er forenlig med amerikansk rett, vil et slikt samarbeid omfatte uavhengige tilsynsorganer (f.eks. generalinspektører) med ansvar for og myndighet til å gjennomføre en grundig undersøkelse (særlig gjennom tilgang til alle relevante dokumenter og myndighet til å anmode om informasjon og uttalelser) og gripe inn ved manglende overholdelse([174]). Privacy Shield-ombudet vil også kunne henvise saker til PCLOB([175]). Dersom et av disse tilsynsorganene konstaterer manglende overholdelse, skal berørte enheter innen etterretningssamfunnet (f.eks. et etterretningsbyrå) korrigere den manglende overholdelsen, ettersom dette er den eneste muligheten ombudet har til å gi

([172]) Dersom klageren ber om innsyn i dokumenter som innehas av amerikanske offentlige myndigheter, får reglene og framgangsmåtene fastsatt i Freedom of Information Act anvendelse. Dette omfatter muligheten til å begjære rettslig prøving (istedenfor uavhengig tilsyn) dersom anmodningen avvises, på vilkårene fastsatt i FOIA.

([173]) I henhold til ombudsmekanismen (vedlegg III, avsnitt 4 bokstav f)) vil Privacy Shield-ombudet kommunisere direkte med EU-klagebehandlingsorganet, som vil ha ansvar for å kommunisere med personen som inngir anmodningen. Dersom direkte kommunikasjon er en del av de «underliggende prosessene» som kan gi den ønskede løsningen (f.eks. en anmodning om innsyn i henhold til FOIA, se avsnitt 5), vil slik kommunikasjon finne sted i samsvar med gjeldende framgangsmåter.

([174]) Se ombudsmekanismen (vedlegg III), avsnitt 2 bokstav a). Se også betraktning 0–0.

([175]) Se ombudsmekanismen (vedlegg III), avsnitt 2 bokstav c). I forklaringene framlagt av den amerikanske regjering skal PCLOB løpende gjennomgå de amerikanske terrorbekjempelsesmyndighetenes retningslinjer og prosedyrer samt gjennomføringen av dette for å bestemme om deres tiltak «i tilstrekkelig grad ivaretar personvernet og de borgerlige frihetsrettighetene og er i samsvar med gjeldende lover, regler og retningslinjer på området personvern og borgerlige frihetsrettigheter.» Det skal også «motta og gjennomgå rapporter og annen informasjon fra ansvarlige for personvern og borgerlige frihetsrettigheter og, dersom det er relevant, utstede anbefalinger til dem om deres aktiviteter.»

personen et «positivt» svar (dvs. at enhver manglende overholdelse er blitt korrigert), som den amerikanske regjering har forpliktet seg til. Som en del av samarbeidet vil Privacy Shield-ombudet bli underrettet om utfallet av undersøkelsen, og ombudet vil ha nødvendige midler for å sikre at det mottar all nødvendig informasjon for å kunne utarbeide sitt svar.

121) Privacy Shield-ombudet vil dessuten være uavhengig av, og vil dermed ikke motta instrukser fra, det amerikanske etterretningssamfunnet([176]). Dette er av vesentlig betydning ettersom ombudet skal «bekrefte» at i) klagen er blitt behørig undersøkt, og at ii) relevant amerikansk rett – herunder især begrensningene og garantiene omhandlet i vedlegg VI – er blitt overholdt, eller at en eventuell manglende overholdelse er blitt korrigert. For å kunne gi denne uavhengige bekreftelsen må Privacy Shield-ombudet motta den nødvendige informasjonen om undersøkelsen for å kunne vurdere nøyaktigheten av svaret på klagen. Den amerikanske utenriksministeren har i tillegg forpliktet seg til å sikre at statssekretæren skal utføre funksjonen som Privacy Shield-ombud på en objektiv måte og uten utilbørlig påvirkning som kan innvirke på svaret som skal gis.

122) Samlet sett sikrer denne mekanismen at individuelle klager vil bli grundig undersøkt og avgjort, og at dette i det minste på området overvåking vil omfatte uavhengige tilsynsorganer med nødvendig ekspertise og undersøkelsesmyndighet og et ombud som vil kunne utføre sine funksjoner uten utilbørlig, særlig politisk, påvirkning. Videre vil privatpersoner kunne inngi klager uten å måtte bevise eller legge fram indikasjoner på at de har vært gjenstand for overvåking([177]). På bakgrunn av disse elementene finner Kommisjonen at det foreligger hensiktsmessige og effektive garantier mot misbruk.

123) På bakgrunn av det ovenstående konkluderer Kommisjonen med at De forente stater sikrer et effektivt rettslig vern mot amerikanske etterretningsmyndigheters inngrep i de grunnleggende rettighetene til personer hvis opplysninger overføres fra Unionen til De forente stater innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater.

124) I denne forbindelse noterer Kommisjonen seg domstolens dom i *Schrems*-saken, der det angis at «lovgivning som ikke inneholder en mulighet for en privatperson til å gjøre bruk av rettsmidler for å få innsyn i personopplysninger som gjelder vedkommende, eller for å få rettet eller slettet slike opplysninger, ikke respekterer det vesentligste innholdet i den grunnleggende retten til et effektivt rettslig vern som nedfelt i artikkel 47 i pakten»([178]). Ifølge Kommisjonens vurdering foreligger det slike rettsmidler i De forente stater, herunder gjennom opprettelse av ombudsmekanismen. Ombudsmekanismen omfatter uavhengig tilsyn med undersøkelsesmyndighet. Mekanismens effektivitet vil bli vurdert på nytt innenfor rammen av Kommisjonens løpende overvåking av Privacy Shield-ordningen, herunder gjennom den årlige felles gjennomgåelsen som også skal omfatte ombudet.

3.2. *Amerikanske offentlige myndigheters tilgang til og bruk av personopplysninger med henblikk på rettshåndheving og formål i allmennhetens interesse*

125) Når det gjelder inngrep i personopplysninger som overføres innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater med henblikk på rettshåndheving, har den amerikanske regjering (gjennom justisdepartementet) lagt fram dokumentasjon om gjeldende begrensninger og garantier som etter Kommisjonens vurdering viser at nivået for vern av personopplysninger er tilstrekkelig.

([176]) Se Roman Zakharov v Russia, dom av 4. desember 2015 (storkammer), saksnr. 47143/06, nr. 275 («selv om det i prinsippet er ønskelig at tilsynsfunksjonen overlates til en dommer, kan ikke-rettslige organers tilsyn anses som forenlig med konvensjonen, forutsatt at tilsynsorganet er uavhengig av myndighetene som utfører tilsynet, og at det har tilstrekkelig og effektiv tilsynsmyndighet»).

([177]) Se Kennedy v the United Kingdom, dom av 18. mai 2010, saksnr. 26839/05, nr. 167.

([178]) Schrems, nr. 95. Som det klart framgår av nr. 91 og 96 i dommen, gjelder nr. 95 det beskyttelsesnivået som garanteres i Unionens rettsorden, og som beskyttelsesnivået i tredjestaten «i hovedtrekk må tilsvare». I henhold til nr. 73 og 74 i dommen krever dette ikke at beskyttelsesnivået eller de midlene som en tredjestat bruker, må være identiske, selv om midlene som skal brukes, i praksis må vise seg å være effektive.

126) Ifølge denne informasjonen kreves det i henhold til det fjerde tillegget til den amerikanske grunnloven([179]) at rettshåndhevende myndigheter([180]) i prinsippet må ha en kjennelse fra en domstol som er avsagt på grunnlag av en «rimelig grunn» for å kunne foreta ransakinger og beslagleggelser. I de få særlige tilfellene og unntakstilfellene der det ikke foreligger krav om kjennelse([181]), er rettshåndhevingen underlagt en «rimelighetstest»([182]). Hvorvidt en ransaking eller beslagleggelse er rimelig, «fastslås ved på den ene side å vurdere i hvilken grad dette griper inn i en persons privatliv, og på den annen side ved å vurdere i hvilken grad dette er nødvendig for å fremme berettigede statlige interesser»([183]). Mer generelt garanterer det fjerde grunnlovstillegget retten til privatliv og verdighet samt beskytter mot vilkårlige og inngripende handlinger fra statstjenestemenn([184]). Disse begrepene gjenspeiler ideen om nødvendighet og forholdsmessighet i unionsretten. Når det i forbindelse med rettshåndheving ikke lenger er bruk for de beslaglagte gjenstandene som bevis, skal de leveres tilbake([185]).

127) Selv om det fjerde grunnlovstillegget ikke omfatter ikke-amerikanske personer som ikke er bosatt i De forente stater, er disse likevel indirekte omfattet av det vernet det gir, ettersom personopplysningene innehas av amerikanske selskaper, noe som innebærer at rettshåndhevende myndigheter i alle tilfeller må søke om rettskjennelse (eller i det minste respektere kravet om rimelighet)([186]). Et ytterligere vern sikres gjennom særlige lovbestemmelser og i det amerikanske justisdepartementets retningslinjer, som begrenser rettshåndhevende myndigheters tilgang til opplysninger til det som tilsvarer prinsippet om nødvendighet og forholdsmessighet (f.eks. ved å kreve at FBI skal bruke minst mulig inngripende etterforskningsmetoder, idet det tas hensyn til den virkningen disse har på personvernet og de borgerlige frihetsrettighetene)([187]). Ifølge redegjørelsene fra den amerikanske regjering gjelder samme eller et høyere vern for rettshåndhevende myndigheters etterforskning på delstatsplan (etterforskning som omfattes av delstatslover)([188]).

128) Selv om en rettslig forhåndsgodkjenning utstedt av en domstol eller storjury (en etterforskningsgren av domstolen utpekt av en dommer eller fredsdommer) ikke er nødvendig i alle tilfeller([189]), er administrative pålegg begrenset til særlige tilfeller og vil bli underlagt uavhengig domstolskontroll, i hvert fall når regjeringen anmoder om å få håndhevet pålegget av domstolen([190]).

([179]) I henhold til det fjerde grunnlovstillegget «skal folkets rett til sikkerhet for egen person, boliger, papirer og eiendeler mot urimelige ransakinger og beslagleggelser ikke krenkes, og det skal ikke avsies kjennelser uten at det foreligger en rimelig grunn understøttet av ed eller forsikring som særlig beskriver stedet som skal ransakes, personene som skal pågripes, eller tingene som skal beslaglegges.» Det er bare dommere som kan utstede ransakingsordrer. Føderale kjennelser om kopiering av elektronisk lagrede opplysninger er underlagt regel 41 i Federal Rules of Criminal Procedure.

([180]) Den amerikanske høyesterett har gjentatte ganger omtalt ransakinger uten ransakingsordrer som «unntak». 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 høyesterett understreker også regelmessig at «den mest grunnleggende konstitusjonelle regelen på dette området er at ransakinger som foretas utenfor rettsprosessen, uten forhåndsgodkjenning fra en dommer, i seg selv er urimelige i henhold til det fjerde grunnlovstillegget – med unntak av et fåtall spesifikt fastsatte og veldefinerte unntak.» 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, avsnitt 215 Report, s. 107, som henviser til Maryland v King, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB, avsnitt 215 Report, s. 107, som henviser 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 av 4.12.2015 (storkammer), saksnr. 47143/06, nr. 269, der det angis at «kravet om at leverandøren av kommunikasjonstjenester skal forevises en tillatelse til oppfanging før det kan oppnås tilgang til en persons kommunikasjon, er en av de viktigste garantiene mot misbruk fra de rettshåndhevende myndighetenes side, og sikrer at det i alle tilfeller av oppfanging innhentes en egnet tillatelse.»

([187]) Justisdepartementets redegjørelser (vedlegg VII), s. 4 med ytterligere henvisninger.

([188]) Justisdepartementets redegjørelser (vedlegg VII), n. 2.

([189]) Ifølge den informasjonen som Kommisjonen har mottatt – dersom det ses bort fra spesifikke områder som trolig ikke er relevante for dataoverføringer innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater (f.eks. etterforskning av misbruk av helsetjenesteytelser, overgrep mot barn eller saker som gjelder kontrollerte stoffer) – gjelder dette hovedsakelig visse myndigheter som omfattes av Electronic Communications Privacy Act (ECPA), nærmere bestemt anmodninger om abonnentopplysninger (18 U.S.C. § 2703 (c) (1), (2), f.eks. adresse, tjenestens type/varighet) og om innholdet i e-postmeldinger som er over 180 dager gamle (18 U.S.C. § 2703 (a), (b)). I sistnevnte tilfelle skal den berørte personen imidlertid underrettes, og vedkommende har dermed mulighet til å bestride anmodningen ved domstolene. Se også oversikten i DOJ, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, kap. 3: The Stored Communications Act, s. 115-138.

([190]) Ifølge redegjørelsene fra den amerikanske regjering kan mottakere av administrative pålegg bestride disse ved domstolene med den begrunnelsen at de er urimelige, dvs. overdrevne, undertrykkende eller tyngende. Se justisdepartementets redegjørelser (vedlegg VII), s. 2.

129) Det samme gjelder bruk av administrative pålegg for formål i allmennhetens interesse. Ifølge redegjørelsene fra den amerikanske regjering får tilsvarende vesentlige begrensninger anvendelse, ettersom byråer bare kan søke om tilgang til opplysninger som er relevante for saker som omfattes av deres myndighet, og skal respektere kriteriet om rimelighet.

130) Videre inneholder amerikansk rett en rekke rettsmidler som privatpersoner kan gjøre gjeldende mot en offentlig myndighet eller en offentlig ansatt i tilfeller der disse myndighetene behandler personopplysninger. Disse rettsmidlene, som særlig omfatter Administrative Procedure Act (APA), Freedom of Information Act (FOIA) og Electronic Communications Privacy Act (ECPA), er tilgjengelige for alle privatpersoner uavhengig av deres statsborgerskap og med forbehold for gjeldende vilkår.

131) I henhold til bestemmelsene om domstolskontroll i Administrative Procedure Act([191]) har «enhver person som lider rettslig urett som følge av et byrås handlinger, eller som er blitt krenket eller forurettet av et byrås handlinger», rett til å anmode om domstolskontroll([192]). Dette omfatter muligheten til å be domstolen om å «erklære ulovlig og sette til side et byrås tiltak, funn og konklusjoner som anses for å være […] vilkårlige, ustadige eller et uttrykk for maktmisbruk, eller som på annen måte ikke er i samsvar med loven»([193]).

132) Mer spesifikt er det i avsnitt II i Electronic Communications Privacy Act([194]) fastsatt en rekke lovbestemte personvernrettigheter som regulerer rettshåndhevende myndigheters tilgang til innhold i trådbasert, muntlig eller elektronisk kommunikasjon som lagres av tredjepartsleverandører([195]). Loven kriminaliserer ulovlig tilgang (dvs. tilgang som ikke er godkjent av en domstol eller tillatt på annen måte) til slik kommunikasjon og gjør det mulig for en berørt privatperson å anlegge sivilt søksmål ved en amerikansk føderal domstol mot en statstjenestemann som forsettlig har begått slike ulovlige handlinger, eller mot De forente stater, for å få tilkjent faktisk skadeserstatning, herunder straffeerstatning, eller for å søke oppreisning eller anerkjennelse.

133) I henhold til Freedom of Information Act (FOIA, 5 U.S.C. § 552) har enhver person også rett til å få innsyn i føderale byråers registre og, når de administrative rettsmidlene er uttømt, til å få fullbyrdet en slik rett ved domstolene, unntatt når slike registre pga. et unntak eller et særlig rettshåndhevingsrelatert fritak er beskyttet mot offentliggjøring([196]).

([191]) 5 U.S.C. § 702.

([192]) På generelt grunnlag er det bare et byrås «endelige» – og ikke «foreløpige, prosedyremessige eller mellomliggende» – tiltak som er gjenstand for domstolskontroll. Se 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706 (2) (A).

([194]) 18 U.S.C. §§ 2701–2712.

([195]) ECPA beskytter kommunikasjon som innehas av to definerte klasser av nettjenesteleverandører, nærmere bestemt leverandører av i) elektroniske kommunikasjonstjenester, f.eks. telefoni eller e-post, ii) fjerndatabehandlingstjenester, f.eks. datalagrings- eller behandlingstjenester.

([196]) Disse unntakene er imidlertid begrensede. I henhold til 5 U.S.C. § 552 (b) (7) er rettigheter i henhold til FOIA f.eks. utelukket for «registre eller informasjon som er samlet inn for rettshåndhevingsformål, men bare i den grad framleggingen av slike rettshåndhevingsregistre eller -informasjon A) med rimelighet kan antas å komme i konflikt med rettshåndhevingstiltak, B) vil frata en person retten til en rettferdig rettergang eller en upartisk dom, C) med rimelighet kan antas å utgjøre en uberettiget krenkelse av privatlivet, D) med rimelighet kan antas å avsløre identiteten til en konfidensiell kilde, herunder en stat, et innen- eller utenlandsk organ eller myndighet eller en privat institusjon som har levert informasjon på konfidensielt grunnlag, og – i tilfelle av et register eller informasjon samlet inn i forbindelse med en strafferettslig etterforskning eller av et organ som utfører en lovlig etterretningsundersøkelse knyttet til nasjonal sikkerhet – informasjon levert av en konfidensiell kilde, E) vil avsløre teknikker og framgangsmåter som rettshåndhevende myndigheter bruker ved etterforskning eller straffeforfølginger, eller vil avsløre retningslinjer som rettshåndhevende myndigheter bruker ved etterforskning eller straffeforfølging, dersom slik avsløring med rimelighet kan antas å medføre en omgåelse av loven, eller F) med rimelighet kan forventes å sette en persons liv eller fysiske sikkerhet i fare.» I tillegg kommer at «når det inngis en anmodning om innsyn i registre hvis framlegging med rimelighet kan antas å komme i konflikt med rettshåndhevingstiltak, og A) undersøkelsen eller prosedyren omfatter en mulig overtredelse av strafferetten og B) det er grunn til å tro at i) vedkommende som er gjenstand for undersøkelsen eller prosedyren, ikke er klar over dens litispendens, og ii) avsløring av at registrene eksisterer med rimelighet kan antas å komme i konflikt med rettshåndhevingstak, kan byrået, utelukkende så lenge omstendighetene varer, behandle registrene som om de ikke var underlagt kravene i dette avsnitt.» (5 U.S.C. § 552 (c) (1)).

134) I tillegg gir en rekke andre lovbestemmelser privatpersoner rett til å anlegge sak mot en amerikansk offentlig myndighet eller offentlig ansatt når det gjelder behandling av deres personopplysninger, f.eks. 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) Kommisjonen konkluderer derfor med at De forente stater har regler som sørger for at eventuelle inngrep for rettshåndhevingsformål([202]) eller andre formål i allmennhetens interesse i de grunnleggende rettighetene til personer hvis personopplysninger overføres fra Unionen til De forente stater innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, begrenses til det som er strengt nødvendig for å nå det aktuelle berettigede målet, og at dette sikrer et effektivt rettslig vern mot slike inngrep.

4. TILSTREKKELIG BESKYTTELSESNIVÅ INNENFOR RAMMEN AV PRIVACY SHIELD-AVTALEN MELLOM EU OG DE FORENTE STATER

136) På bakgrunn av disse konstateringene anser Kommisjonen at De forente stater sikrer et tilstrekkelig nivå for vern av personopplysninger som overføres fra Unionen til egensertifiserte organisasjoner i De forente stater innenfor rammen av Privacy Shield-avtal0065n mellom EU og De forente stater.

137) Kommisjonen anser særlig at prinsippene utstedt av det amerikanske handelsdepartementet i det store og hele sikrer et nivå for vern av personopplysninger som i hovedtrekk tilsvarer det som garanteres av de grunnleggende prinsippene fastsatt i direktiv 95/46/EF.

138) En effektiv anvendelse av prinsippene er dessuten garantert ved kravene til åpenhet samt det amerikanske handelsdepartementets forvaltning av Privacy Shield-avtalen.

139) Kommisjonen mener videre at Privacy Shield-ordningens mekanismer for tilsyn og klageadgang gjør det mulig å identifisere overtredelser av prinsippene begått av Privacy Shield-organisasjoner og å straffe disse i praksis, samt sikre de registrerte rettsmidler slik at de kan få innsyn i personopplysninger som gjelder dem, og eventuelt få rettet eller slettet slike opplysninger.

140) På bakgrunn av tilgjengelig informasjon om De forente staters rettsorden, herunder den amerikanske regjerings redegjørelser og forpliktende tilsagn, anser Kommisjonen at eventuelle inngrep fra amerikanske offentlige myndigheter i de grunnleggende rettighetene til personer hvis personopplysninger overføres fra Unionen til De forente stater innenfor rammen av Privacy Shield-ordningen for formål knyttet til nasjonal sikkerhet, rettshåndheving eller andre formål i allmennhetens interesse, samt de påfølgende begrensningene som er pålagt egensertifiserte organisasjoner når det gjelder deres tilslutning til prinsippene, vil være begrenset til det som er strengt nødvendig for å nå det aktuelle berettigede målet, og at det foreligger et effektivt rettslig vern mot slike inngrep.

([197]) 18 U.S.C. §§ 2510 et seq. I henhold til Wiretap Act (18 U.S.C. § 2520) kan en person hvis trådbaserte, muntlige eller elektroniske kommunikasjon oppfanges, offentliggjøres eller bevisst brukes, anlegge sivilt søksmål for overtredelse av Wiretap Act, herunder under visse omstendigheter mot en individuell statstjenestemann eller De forente stater. Når det gjelder innsamling av adresseopplysninger og andre innholdsløse opplysninger (f.eks. IP-adresse, e-postadresse til/fra), se også kapittelet «Pen Registers and Trap and Trace Devices» i Title 18 (18 U.S.C. §§ 3121–3127 og angående sivile søksmål § 2707).

([198]) 18 U.S.C. § 1030. I henhold til Computer Fraud and Abuse Act kan en person anlegge sak mot en annen person for bevisst uautorisert tilgang (eller tilgang ut over autorisert tilgang) for å innhente opplysninger fra en finansinstitusjon, et statlig databehandlingssystem eller en annen angitt datamaskin, herunder under visse omstendigheter mot en individuell statstjenestemann.

([199]) 28 U.S.C. §§ 2671 et seq. I henhold til Federal Tort Claims Act kan en person under visse omstendigheter anlegge sak mot De forente stater for «uaktsomme eller ulovlige handlinger eller utelatelser som begås av en statstjenestemann i forbindelse med vedkommendes funksjoner eller arbeid.»

([200]) 12 U.S.C. §§ 3401 et seq. I henhold til Right to Financial Privacy Act kan en person under visse omstendigheter anlegge sak mot De forente stater for å få tilgang til eller utlevert beskyttede finansielle dokumenter i strid med loven. Offentlige myndigheters tilgang til beskyttede finansielle dokumenter er generelt sett forbudt, med mindre anmodningen gjøres på grunnlag av en lovlig stevning eller ransakingsordre eller, med visse begrensninger, en formell skriftlig anmodning som personen som opplysningene gjelder, underrettes om.

([201]) 15 U.S.C. §§ 1681–1681x. I henhold til Fair Credit Reporting Act kan en person anlegge sak mot enhver person som ikke overholder kravene (særlig behovet for lovlig godkjenning) til innsamling, spredning og bruk av forbrukerkredittrapporter eller, under visse omstendigheter, mot en offentlig etat.

([202]) Domstolen har anerkjent at rettshåndheving utgjør et berettiget politisk mål. Se forente saker C-293/12 og C-594/12, Digital Rights Ireland and Others, EU:C:2014:238, nr. 42. Se også artikkel 8 nr. 2 i ECHR og Den europeiske menneskerettighetsdomstols dom i saken Weber and Saravia v Germany, saksnr. 54934/00, nr. 104.

141) Kommisjonen konkluderer med at dette oppfyller standardene i artikkel 25 i direktiv 95/46/EF tolket på bakgrunn av Den europeiske unions pakt om grunnleggende rettigheter, som forklart av Domstolen, særlig i *Schrems*-dommen.

5. PERSONVERNMYNDIGHETENES TILTAK OG INFORMASJON TIL KOMMISJONEN

142) I *Schrems*-dommen presiserte Domstolen at Kommisjonen ikke har kompetanse til å begrense den myndigheten som personvernmyndigheter har i henhold til artikkel 28 i direktiv 95/46/EF (herunder myndigheten til å innstille dataoverføringer) dersom en person i forbindelse med en klage i henhold til denne bestemmelse reiser tvil om hvorvidt en kommisjonsbeslutning om tilstrekkelig beskyttelsesnivå er forenlig med vernet av den grunnleggende retten til privatliv og vern av personopplysninger([203]).

143) For å sikre et effektivt tilsyn med hvordan Privacy Shield-ordningen fungerer bør medlemsstatene underrette Kommisjonen om relevante tiltak truffet av personvernmyndighetene.

144) Domstolen anså videre at medlemsstatene og deres organer, i tråd med artikkel 25 nr. 6 annet ledd i direktiv 95/46/EF, skal treffe de tiltakene som er nødvendige for å overholde EU-institusjonenes rettsakter, ettersom disse i prinsippet antas å være lovlige og dermed har rettsvirkning så lenge de ikke er trukket tilbake, opphevet innenfor rammen av en opphevingssak eller er erklært ugyldige som følge av en begjæring om forhåndsavgjørelse eller en påstand om rettsstridighet. En kommisjonsbeslutning om tilstrekkelig beskyttelsesnivå truffet i henhold til artikkel 25 nr. 6 i direktiv 95/46/EF er derfor bindende for alle organer i medlemsstatene som den er rettet til, herunder deres uavhengige tilsynsmyndigheter([204]). Dersom en slik myndighet har mottatt en klage som reiser tvil om hvorvidt en kommisjonsbeslutning om tilstrekkelig beskyttelsesnivå er forenlig med vernet av den grunnleggende retten til privatliv og vern av personopplysninger, og myndigheten finner at klagepunktene er velbegrunnede, skal det i nasjonal rett foreligge rettsmidler som gjør det mulig å bringe nevnte klagepunkter inn for en nasjonal domstol, som ved tvil skal utsette saken og framsette en begjæring om forhåndsavgjørelse for Domstolen([205]).

6. REGELMESSIG GJENNOMGÅELSE AV KONSTATERINGEN AV TILSTREKKELIG BESKYTTELSESNIVÅ

145) Ettersom nivået for vern av personopplysninger som De forente staters rettsorden sikrer, kan endres, vil Kommisjonen etter å ha truffet denne beslutning regelmessig kontrollere om konstateringen av at De forente stater sikrer et tilstrekkelig beskyttelsesnivå innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, fremdeles er saklig og rettslig begrunnet. En slik kontroll skal under alle omstendigheter foretas dersom Kommisjonen mottar informasjon som reiser begrunnet tvil om dette([206]).

146) Kommisjonen vil derfor løpende overvåke det overordnede rammeverket for overføring av personopplysninger som opprettes ved Privacy Shield-avtalen mellom EU og De forente stater, samt at amerikanske myndigheter opptrer i samsvar med redegjørelsene og overholder de forpliktende tilsagnene i dokumentene som er vedlagt denne beslutning. For å forenkle denne prosessen har De forente stater forpliktet seg til å underrette Kommisjonen om vesentlige endringer i amerikansk rett som er relevante for Privacy Shield-ordningen, og som gjelder vern av personopplysninger og de begrensningene og garantiene som gjelder for offentlige myndigheters tilgang til personopplysninger. Videre vil denne beslutning bli gjenstand for en årlig felles gjennomgåelse som vil omfatte alle aspekter av hvordan Privacy Shield-avtalen mellom EU og De forente stater fungerer, herunder unntakene fra prinsippene knyttet til nasjonal sikkerhet og rettshåndheving. Ettersom konstateringen av at nivået for vern av personopplysninger er tilstrekkelig også kan bli påvirket av utviklingen i unionsretten, vil Kommisjonen vurdere beskyttelsesnivået som Privacy Shield-ordningen gir, etter at den generelle personvernforordningen har trådt i kraft.

147) Med henblikk på den årlige felles gjennomgåelsen nevnt i vedlegg I, II og VI vil det bli avholdt et møte mellom Kommisjonen og det amerikanske handelsdepartementet og FTC, eventuelt ledsaget av andre departementer og byråer som er involvert i gjennomføringen av Privacy Shield-ordningen, samt, i spørsmål som gjelder nasjonal sikkerhet, representanter for ODNI, andre enheter innen etterretningssamfunnet og ombudet. Møtet vil være åpent for EUs personvernmyndigheter og representanter for artikkel 29-arbeidsgruppen.

([203]) Schrems, nr. 40 et seq., 101–103.
([204]) Schrems, nr. 51, 52 og 62.
([205]) Schrems, nr. 65.
([206]) Schrems, nr. 76.

148) I forbindelse med den årlige felles gjennomgåelsen vil Kommisjonen be det amerikanske handelsdepartementet om å legge fram omfattende informasjon om alle relevante aspekter av hvordan Privacy Shield-avtalen mellom EU og De forente stater fungerer, herunder om saker som handelsdepartementet har mottatt fra personvernmyndigheter, og resultatene av *ex officio*-kontroller av om prinsippene overholdes. Kommisjonen vil også prøve å få avklart eventuelle spørsmål eller saker vedrørende Privacy Shield-avtalen mellom EU og De forente stater og måten den fungerer på, som har oppstått som følge av tilgjengelig informasjon, herunder innsynsrapporter som er tillatt i henhold til USA FREEDOM Act, offentlige rapporter fra amerikanske nasjonale etterretningsmyndigheter, personvernmyndighetene, personverngrupper, medierapporter eller andre mulige kilder. For å lette Kommisjonens oppgave i denne forbindelse bør medlemsstatene også underrette Kommisjonen om tilfeller der tiltak truffet av organer med ansvar for å sikre overholdelse av prinsippene i De forente stater, ikke sikrer overholdelse, og om eventuelle tegn på at tiltak truffet av amerikanske offentlige myndigheter med ansvar for nasjonal sikkerhet eller forebygging, etterforskning, avsløring eller straffeforfølging av straffbare forhold, ikke sikrer det nødvendige beskyttelsesnivået.

149) Kommisjonen vil på grunnlag av den årlige felles gjennomgåelsen utarbeide en offentlig rapport som skal framlegges for Europaparlamentet og Rådet.

7. MIDLERTIDIG OPPHEVING AV BESLUTNINGEN OM TILSTREKKELIG BESKYTTELSESNIVÅ

150) Dersom Kommisjonen på grunnlag av kontroller eller annen tilgjengelig informasjon konkluderer med at det beskyttelsesnivået som Privacy Shield-ordningen gir, ikke lenger i hovedtrekk tilsvarer nivået i Unionen, eller dersom det er klare tegn på at det ikke lenger kan sikres at prinsippene overholdes på en effektiv måte i De forente stater, eller at tiltak truffet av amerikanske offentlige myndigheter med ansvar for nasjonal sikkerhet eller forebygging, etterforskning, avsløring eller straffeforfølging av straffbare forhold, ikke sikrer det nødvendige beskyttelsesnivået, vil Kommisjonen underrette det amerikanske handelsdepartementet om dette og anmode om at det treffes egnede tiltak for raskt å korrigere en potensiell manglende overholdelse av prinsippene innen en fastsatt rimelig tidsramme. Dersom amerikanske myndigheter etter utløpet av den fastsatte tidsrammen ikke på en tilfredsstillende måte viser at Privacy Shield-avtalen mellom EU og De forente stater fortsatt sikrer en effektiv overholdelse av prinsippene og et tilstrekkelig beskyttelsesnivå, vil Kommisjonen innlede prosedyren som vil føre til en delvis eller fullstendig midlertidig oppheving eller oppheving av denne beslutning([207]). Alternativt kan Kommisjonen foreslå å endre denne beslutning, f.eks. ved å begrense konstateringen av at beskyttelsesnivået er tilstrekkelig til bare å gjelde dataoverføringer underlagt ytterligere vilkår.

151) Kommisjonen vil særlig innlede prosedyren for midlertidig oppheving eller oppheving

a) ved tegn på at amerikanske myndigheter ikke overholder redegjørelsene og de forpliktende tilsagnene angitt i dokumentene vedlagt denne beslutning, herunder vilkårene og begrensningene som gjelder amerikanske offentlige myndigheters tilgang til personopplysninger som er overført innenfor rammen av Privacy Shield-ordningen, for formål knyttet til rettshåndheving, nasjonal sikkerhet og andre formål i allmennhetens interesse,

b) ved manglende effektiv behandling av klager fra registrerte i EU. I denne forbindelse vil Kommisjonen ta hensyn til alle forhold som påvirker den muligheten registrerte i EU har til å gjøre sine rettigheter gjeldende, herunder særlig de frivillige forpliktende tilsagnene fra egensertifiserte amerikanske selskaper om å samarbeide med personvernmyndighetene og følge deres råd, eller

c) dersom Privacy Shield-ombudet ikke gir rettidige og egnede svar på anmodninger fra registrerte i EU.

152) Kommisjonen vil også vurdere å innlede prosedyren som fører til endring, midlertidig oppheving eller oppheving av denne beslutning dersom, i forbindelse med den årlige felles gjennomgåelsen av hvordan Privacy Shield-avtalen mellom EU og De forente stater fungerer, det amerikanske handelsdepartementet eller andre departementer eller byråer som er involvert i gjennomføringen av Privacy Shield-ordningen, eller ved spørsmål som gjelder nasjonal sikkerhet, representanter for det amerikanske etterretningssamfunnet eller ombudet ikke legger fram den informasjonen eller de

([207]) Fra og med anvendelsesdatoen for den generelle personvernforordningen vil Kommisjonen bruke sin myndighet til i behørig begrunnede, tvingende hastetilfeller å vedta en gjennomføringsrettsakt som midlertidig opphever denne beslutning, og som får anvendelse umiddelbart uten at den først framlegges for den berørte komitologikomiteen, og som skal gjelde i høyst seks måneder.

presiseringene som er nødvendige for å kunne vurdere overholdelsen av prinsippene, klagebehandlingsprosedyrenes effektivitet eller en eventuell reduksjon i det nødvendige nivået for vern av personopplysninger som følge av tiltak truffet av amerikanske nasjonale etterretningsmyndigheter, særlig som følge av innsamling og/eller tilgang til personopplysninger som ikke er begrenset til det som er strengt nødvendig og forholdsmessig. I denne forbindelse vil Kommisjonen ta hensyn til i hvilket omfang den relevante informasjonen kan innhentes fra andre kilder, herunder rapporter fra egensertifiserte amerikanske selskaper i henhold til USA FREEDOM Act.

153) Arbeidsgruppen for personvern i forbindelse med behandling av personopplysninger nedsatt ved artikkel 29 i direktiv 95/46/EF har avgitt uttalelse om det nivået for vern av personopplysninger som sikres ved Privacy Shield-avtalen mellom EU og De forente stater([208]), som det er tatt hensyn til ved utarbeidingen av denne beslutning.

154) Europaparlamentet har vedtatt en resolusjon om transatlantiske datastrømmer([209]).

155) Tiltakene fastsatt i denne beslutning er i samsvar med uttalelse fra komiteen nedsatt ved artikkel 31 nr. 1 i direktiv 95/46/EF.

TRUFFET DENNE BESLUTNING:

Artikkel 1

1. Med hensyn til artikkel 25 nr. 2 i direktiv 95/46/EF sikrer De forente stater et tilstrekkelig nivå for vern av personopplysninger som overføres fra Unionen til organisasjoner i De forente stater innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater.

2. Privacy Shield-avtalen mellom EU og De forente stater består av prinsippene utstedt av det amerikanske handelsdepartementet 7. juli 2016 som fastsatt i vedlegg II, og de offisielle redegjørelsene og forpliktende tilsagnene angitt i dokumentene i vedlegg I og III–VII.

3. Med henblikk på nr. 1 overføres personopplysninger innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater når de overføres fra Unionen til organisasjoner i De forente stater som er oppført på «Privacy Shield-listen», som føres og offentliggjøres av det amerikanske handelsdepartementet, i samsvar med avsnitt I og III i prinsippene omhandlet i vedlegg II.

Artikkel 2

Denne beslutning berører ikke anvendelsen av bestemmelsene i direktiv 95/46/EF, bortsett fra artikkel 25 nr. 1 som gjelder behandling av personopplysninger i medlemsstatene, særlig artikkel 4.

Artikkel 3

Når vedkommende myndigheter i medlemsstatene utøver sin myndighet i henhold til artikkel 28 nr. 3 i direktiv 95/46/EF, og dette fører til en midlertidig innstilling av eller endelig forbud mot datastrømmer til en organisasjon i De forente stater som er oppført på Privacy Shield-listen i samsvar med avsnitt I og III i prinsippene omhandlet i vedlegg II, med det formål å beskytte privatpersoner i forbindelse med behandling av deres personopplysninger, skal de berørte medlemsstatene uten opphold underrette Kommisjonen.

Artikkel 4

1. Kommisjonen vil løpende overvåke hvordan Privacy Shield-avtalen mellom EU og De forente stater fungerer med henblikk på å vurdere om De forente stater fortsatt sikrer et tilstrekkelig nivå for vern av personopplysninger som i henhold til avtalen overføres fra Unionen til organisasjoner i De forente stater.

([208]) Uttalelse 1/2016 om Privacy Shield-avtalen mellom EU og De forente stater – utkast til beslutning om tilstrekkelig beskyttelsesnivå, vedtatt 13. april 2016.

([209]) Europaparlamentets resolusjon av 26. mai 2016 om transatlantiske datastrømmer (2016/2727(RSP)).

2. Medlemsstatene og Kommisjonen skal underrette hverandre om tilfeller der offentlige organer i De forente stater med lovfestet myndighet til å sikre overholdelse av prinsippene omhandlet i vedlegg II tilsynelatende ikke har innført effektive avsløring- og tilsynsmekanismer som gjør det mulig å identifisere og straffe overtredelser av prinsippene i praksis.

3. Medlemsstatene og Kommisjonen skal underrette hverandre om tegn på at amerikanske offentlige myndigheter med ansvar for nasjonal sikkerhet, rettshåndheving eller andre formål i allmennhetens interesse griper inn i den enkeltes rett til vern av egne personopplysninger ut over det som er strengt nødvendig, og/eller på at det ikke foreligger et effektivt rettslig vern mot slike inngrep.

4. Senest ett år fra den datoen denne beslutning er meddelt medlemsstatene og deretter årlig, skal Kommisjonen vurdere konklusjonene i artikkel 1 nr. 1 på grunnlag av all tilgjengelig informasjon, herunder informasjon mottatt som ledd i den årlige felles gjennomgåelsen omhandlet i vedlegg I, II og VI.

5. Kommisjonen skal legge fram en rapport om relevante konklusjoner for komiteen nedsatt ved artikkel 31 i direktiv 95/46/EF.

6. Kommisjonen skal legge fram et utkast til tiltak i samsvar med framgangsmåten i artikkel 31 nr. 2 i direktiv 95/46/EF med henblikk på en midlertidig oppheving, endring eller oppheving av denne beslutning eller begrensning av dens virkeområde, blant annet ved tegn på

— at amerikanske offentlige myndigheter ikke retter seg etter redegjørelsene og de forpliktende tilsagnene i dokumentene vedlagt denne beslutning, herunder vilkårene og begrensningene som gjelder amerikanske offentlige myndigheters tilgang til personopplysninger som er overført innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater med henblikk på rettshåndheving, nasjonal sikkerhet og andre formål i allmennhetens interesse,

— systematisk manglende effektiv behandling av klager fra registrerte i EU eller

— at Privacy Shield-ombudet systematisk unnlater å svare rettidig og på egnet måte på anmodninger fra registrerte i EU, som påkrevd i avsnitt 4 bokstav e) i vedlegg III.

Kommisjonen vil også legge fram nevnte utkast til tiltak dersom manglende samarbeid mellom organene som skal sikre at Privacy Shield-avtalen mellom EU og De forente stater fungerer i De forente stater, hindrer Kommisjonen i å fastslå om konklusjonene i artikkel 1 nr. 1 er berørt.

Artikkel 5

Medlemsstatene skal treffe alle nødvendige tiltak for å etterkomme denne beslutning.

Artikkel 6

Denne beslutning er rettet til medlemsstatene.

Utferdiget i Brussel 12. juli 2016.

For Kommisjonen

Věra JOUROVÁ

Medlem av Kommisjonen

VEDLEGG I

Brev fra Penny Pritzker, De forente staters handelsminister

7. juli 2016

Věra Jourová
Kommissær for justis, forbrukersaker og likestilling
Europakommisjonen
Rue de la Loi / Westraat 200
1049 Brussel
Belgia

Kjære kommissær Jourová

På vegne av De forente stater har jeg med dette gleden av å oversende en pakke med dokumenter om Privacy Shield-avtalen mellom EU og De forente stater som er resultatet av to års utbytterike drøftinger mellom våre team. Denne pakken utgjør sammen med annet materiale som Kommisjonen har tilgang til via offentlige kilder, et svært solid grunnlag for en ny kommisjonsbeslutning om tilstrekkelig beskyttelsesnivå([1]).

Vi har begge grunn til å være stolte av forbedringene av rammeverket. Privacy Shield-avtalen bygger på prinsipper som det er sterk enighet om på begge sider av Atlanteren, og som vi har styrket. Gjennom vårt samarbeid har vi en reell mulighet til å bedre personvernet over hele verden.

Privacy Shield-pakken inneholder Privacy Shield-prinsippene sammen med et brev (vedlagt som vedlegg 1) fra International Trade Administration (ITA) i det amerikanske handelsdepartementet, som forvalter programmet, der det redegjøres for de forpliktelsene vårt departement har inngått for å sikre at Privacy Shield-ordningen skal fungere effektivt. Pakken inneholder også vedlegg 2, som omfatter handelsdepartementets andre forpliktende tilsagn knyttet til den nye voldgiftsmodellen i Privacy Shield-ordningen.

Jeg har anmodet mine medarbeidere om å sette av alle nødvendige ressurser for å sikre en rask og fullstendig gjennomføring av Privacy Shield-ordningen og for å sikre at forpliktelsene i vedlegg 1 og 2 oppfylles i rett tid.

Privacy Shield-pakken inneholder også andre dokumenter fra andre amerikanske myndigheter, nærmere bestemt:

— Et brev fra Federal Trade Commission (FTC) der det redegjøres for FTCs håndheving av Privacy Shield-ordningen.

— Et brev fra det amerikanske transportdepartementet der det redegjøres for deres håndheving av Privacy Shield-ordningen.

— To brev fra Office of the Director of National Intelligence (ODNI) om de garantiene og begrensningene som gjelder for amerikanske nasjonale sikkerhetsmyndigheter.

— Et brev fra det amerikanske utenriksdepartementet sammen med et memorandum der det redegjøres for at utenriksdepartementet har forpliktet seg til å opprette et nytt Privacy Shield-ombud som henvendelser om amerikansk signaletterretningspraksis kan rettes til.

— Et brev fra det amerikanske justisdepartementet om de garantiene og begrensningene som gjelder for den amerikanske regjerings tilgang med henblikk på rettshåndheving og formål i allmennhetens interesse.

Dere kan være sikre på at De forente stater tar disse forpliktelsene på alvor.

([1]) Forutsatt at kommisjonsbeslutningen om tilstrekkelig beskyttelsesnivå som sikres ved Privacy Shield-avtalen mellom EU og De forente stater, får anvendelse på Island, Liechtenstein og Norge, vil Privacy Shield-pakken omfatte både Den europeiske union og disse tre statene.

Senest 30 dager etter den endelige godkjenningen av beslutningen om tilstrekkelig beskyttelsesnivå, vil hele Privacy Shield-pakken bli levert til *Federal Register* med henblikk på offentliggjøring.

Vi ser fram til å samarbeide om gjennomføringen av Privacy Shield-ordningen når vi nå sammen innleder den neste fasen i denne prosessen.

Vennlig hilsen

Penny Pritzker

———

Vedlegg 1

Brev fra Ken Hyatt, fungerende statssekretær for internasjonal handel

Věra Jourová
Kommissær for justis, forbrukersaker og likestilling
Europakommisjonen
Rue de la Loi / Westraat 200
1049 Brussel
Belgia

Kjære kommissær Jourová

På vegne av International Trade Administration er jeg glad for å kunne redegjøre for det forbedrede vernet av personopplysninger som sikres ved Privacy Shield-avtalen mellom EU og De forente stater (heretter kalt «Privacy Shield-ordningen» eller «ordningen»), og de forpliktelsene det amerikanske handelsdepartementet («departementet») har inngått for å sikre at Privacy Shield-ordningen skal fungere effektivt. Det at vi nå er kommet i mål med denne historiske ordningen er et svært viktig framskritt både for personvernet og for virksomheter på begge sider av Atlanteren. Det gir privatpersoner i EU tillit til at deres personopplysninger vil bli beskyttet, og at de vil ha tilgang til rettsmidler ved eventuelle problemer. Det gir en sikkerhet som vil bidra til vekst i den transatlantiske økonomien ved å sikre at flere tusen europeiske og amerikanske virksomheter fortsatt kan investere og gjøre forretninger på tvers av våre landegrenser. Privacy Shield-ordningen er et resultat av over to års hardt arbeid og samarbeid med dere – våre kolleger i Europakommisjonen («Kommisjonen»). Vi ser fram til et fortsatt samarbeid med Kommisjonen for å sikre at Privacy Shield-ordningen funger etter hensikten.

Vi har samarbeidet med Kommisjonen om utviklingen av Privacy Shield-ordningen, slik at organisasjoner som er etablert i De forente stater, kan oppfylle kravene til tilstrekkelig vern av personopplysninger i henhold til EU-retten. Den nye ordningen innebærer en rekke vesentlige fordeler for både privatpersoner og virksomheter. For det første inneholder den en rekke viktige bestemmelser om vern av personopplysningene til privatpersoner i EU. Den krever at amerikanske organisasjoner som deltar i ordningen, utarbeider et overensstemmende personvernprogram, offentlig forplikter seg til å overholde Privacy Shield-prinsippene slik at forpliktelsen kan kreves oppfylt i henhold til amerikansk rett, årlig foretar en ny sertifisering ved departementet om sin tilslutning til prinsippene, gir privatpersoner i EU tilgang til gratis uavhengig tvisteløsning og er underlagt myndigheten til De forente staters Federal Trade Commission («FTC»), det amerikanske transportdepartementet eller et annet rettshåndhevende organ. For det andre vil Privacy Shield-ordningen gi tusenvis av selskaper i De forente stater og datterselskaper av europeiske selskaper i De forente stater mulighet til å motta personopplysninger fra Den europeiske union og på den måten fremme datastrømmer som vil støtte den transatlantiske handelen. De transatlantiske økonomiske forbindelsene er allerede verdens største og står for halvparten av den globale økonomiske produksjonen, genererer nærmere en billion dollar i handel med varer og tjenester og støtter dermed millioner av arbeidsplasser på begge sider av Atlanteren. Virksomheter som er avhengige av transatlantiske datastrømmer, finnes i alle sektorer og omfatter både store Fortune 500-selskaper og en rekke små og mellomstore bedrifter (SMB). Transatlantiske datastrømmer gjør det mulig for amerikanske organisasjoner å behandle opplysninger som er nødvendige for å kunne tilby varer, tjenester og karrieremuligheter til privatpersoner i EU. Privacy Shield-ordningen er basert på felles personvernprinsipper og bidrar til å bygge bro mellom våre ulike rettssystemer samtidig som den bidrar til å oppfylle handelsmessige og økonomiske mål i både Europa og De forente stater.

Et selskap bestemmer frivillig om det skal slutte seg til den nye ordningen gjennom egensertifisering, men dersom et selskap offentlig forplikter seg til å følge prinsippene i Privacy Shield-ordningen, kan enten Federal Trade Commission eller det amerikanske transportdepartementet, avhengig av hvem som har myndighet over Privacy Shield-organisasjonen, kreve forpliktelsen oppfylt i henhold til amerikansk rett.

Privacy Shield-prinsippene – forbedringer

Den nye Privacy Shield-ordningen styrker personvernet ved å

— kreve at privatpersoner gis mer informasjon i henhold til prinsippet om opplysningsplikt, herunder en erklæring om at organisasjonen deltar i Privacy Shield-ordningen, en uttalelse om privatpersoners rett til å få innsyn i personopplysningene og angivelse av det relevante uavhengige tvisteløsningsorganet,

— styrke vernet av personopplysninger som overføres fra en Privacy Shield-organisasjon til en behandlingsansvarlig tredjepart, ved å kreve at partene inngår en avtale om at nevnte opplysninger bare kan behandles for begrensede og spesifikke formål som privatpersonen har samtykket i, og at mottakeren vil sikre det samme beskyttelsesnivået som det som sikres i prinsippene,

— styrke vernet av personopplysninger som overføres fra en Privacy Shield-organisasjon til en tredjepart som fungerer som representant, herunder ved å kreve at nevnte organisasjon treffer rimelige og egnede tiltak for å sikre at representanten faktisk behandler de overførte personopplysningene i samsvar med organisasjonens forpliktelser i henhold til prinsippene, at den omgående treffer rimelige og egnede tiltak for å stoppe og korrigere uautorisert behandling etter å ha blitt varslet om dette, og på anmodning legger fram for departementet et sammendrag eller en representativ kopi av de relevante personvernbestemmelsene i avtalen med nevnte representant,

— fastsette at en Privacy Shield-organisasjon er ansvarlig for behandlingen av de personopplysningene den mottar innenfor rammen av Privacy Shield-ordningen og deretter overfører til en tredjepart som fungerer som representant på dens vegne, og at nevnte organisasjon skal være ansvarlig i henhold til prinsippene dersom representanten behandler nevnte personopplysninger i strid med prinsippene, med mindre organisasjonen beviser at den ikke er ansvarlig for hendelsen som forvoldte skaden,

— presisere at Privacy Shield-organisasjoner skal begrense personopplysninger til opplysninger som er relevante for formålet med behandlingen,

— kreve at en organisasjon årlig foretar en sertifisering ved departementet om at den forplikter seg til å anvende prinsippene på opplysninger den mottok mens den deltok i Privacy Shield-ordningen, dersom den forlater Privacy Shield-ordningen og velger å beholde nevnte opplysninger,

— kreve at registrerte får gratis tilgang til uavhengige klagemekanismer,

— kreve at organisasjoner og deres utvalgte uavhengige klagemekanismer omgående besvarer henvendelser og forespørsler fra departementet om informasjon knyttet til Privacy Shield-ordningen,

— kreve at organisasjoner svarer raskt på klager på manglende overholdelse av prinsippene henvist via departementet fra EU-medlemsstatene, og

— kreve at en Privacy Shield-organisasjon offentliggjør alle relevante Privacy Shield-relaterte avsnitt i overholdelses- eller vurderingsrapporter som legges fram for FTC dersom den blir gjenstand for en FTC-avgjørelse eller en rettsavgjørelse om manglende overholdelse.

Handelsdepartementets forvaltning av og tilsyn med Privacy Shield-ordningen

Departementet gjentar at det har forpliktet seg til å føre og offentliggjøre en offisiell liste over amerikanske organisasjoner som ved egensertifisering ved departementet har forpliktet seg til å overholde prinsippene (heretter kalt «Privacy Shield-listen»). Departementet vil sørge for å holde Privacy Shield-listen oppdatert ved å fjerne organisasjoner som frivillig trekker seg, ikke foretar den årlige nye sertifiseringen i samsvar med departementets framgangsmåter eller som vedvarende ikke overholder prinsippene. Departementet vil også føre og offentliggjøre en offisiell fortegnelse over amerikanske organisasjoner som tidligere har foretatt egensertifisering ved departementet, men som er blitt fjernet fra Privacy Shield-listen, herunder de som er blitt fjernet på grunn av vedvarende manglende overholdelse av prinsippene. Departementet vil opplyse om hvorfor den enkelte organisasjon er blitt fjernet.

Departementet forplikter seg også til å styrke forvaltningen av og tilsynet med Privacy Shield-ordningen. Departementet vil særlig

angi ytterligere opplysninger på Privacy Shield-nettstedet,

— opprette Privacy Shield-listen samt en fortegnelse over de organisasjonene som ved egensertifisering tidligere har erklært at de har sluttet seg til prinsippene, men som ikke lenger kan nyte godt av fordelene ved Privacy Shield-ordningen,

— på et framtredende sted angi at alle organisasjoner som er blitt fjernet fra Privacy Shield-listen, ikke lenger kan nyte godt av fordelene ved Privacy Shield-ordningen, men likevel skal fortsette å anvende prinsippene på personopplysningene de mottok mens de deltok i Privacy Shield-ordningen, så lenge de er i besittelse av nevnte opplysninger, og

— angi en lenke til listen over Privacy Shield-relaterte FTC-saker på FTCs nettsted.

Kontroll av egensertifiseringskrav

— før en organisasjons egensertifisering (eller den årlige nye sertifiseringen) fullføres, og før organisasjonen oppføres på Privacy Shield-listen, kontrollere at organisasjonen

  — har angitt de nødvendige kontaktopplysningene til organisasjonen,

  — har beskrevet organisasjonens aktiviteter med hensyn til personopplysninger som mottas fra EU,

  — har angitt hvilke personopplysninger som omfattes av organisasjonens egensertifisering,

  — dersom organisasjonen har et offentlig nettsted, har angitt nettadressen der personvernprogrammet er tilgjengelig, og at det er tilgjengelig på den angitte nettadressen, eller dersom en organisasjon ikke har et offentlig nettsted, har angitt hvor allmennheten kan få tilgang til personvernprogrammet,

  — har angitt i sitt relevante personvernprogram at den har sluttet seg til prinsippene, og, dersom personvernprogrammet er tilgjengelig på nettet, har angitt en hyperlenke til departementets Privacy Shield-nettsted,

  — har angitt det spesifikke lovfestede organet med myndighet til å behandle klager på organisasjonen som gjelder urimelig eller villedende praksis eller brudd på personvernlover og -forskrifter (og som er angitt i prinsippene eller i et framtidig vedlegg til prinsippene),

  — dersom organisasjonen velger å oppfylle kravene i bokstav a) i) og a) iii) i prinsippet om klageadgang, håndheving og ansvar ved å forplikte seg til å samarbeide med egnede personvernmyndigheter i EU, har angitt at den akter å samarbeide med personvernmyndighetene for å undersøke og avgjøre klager mottatt innenfor rammen av Privacy Shield-ordningen, særlig svare på forespørsler fra disse, i tilfeller der registrerte i EU har inngitt klager direkte til nasjonale personvernmyndigheter,

  — har angitt de personvernprogrammene som organisasjonen deltar i,

  — har angitt hvilke metoder som brukes til å kontrollere at prinsippene overholdes (f.eks. internkontroll, kontroll utført av en tredjepart),

  — har angitt, både i sin egensertifiseringsmelding og i sitt personvernprogram, hvilken uavhengig klagemekanisme som er tilgjengelig for å undersøke og avgjøre klager,

  — har angitt i sitt relevante personvernprogram, dersom det er tilgjengelig på nettet, en hyperlenke til nettstedet eller klageskjemaet til den uavhengige klagemekanismen med ansvar for å behandle uløste klager, og

  — dersom organisasjonen har angitt at den akter å få overført opplysninger om menneskelige ressurser fra EU til bruk i forbindelse med et arbeidsforhold, har erklært at den vil samarbeide med og rette seg etter personvernmyndighetene for å avgjøre klager på organisasjonens aktiviteter i forbindelse med slike opplysninger, har framlagt for departementet en kopi av sitt personvernprogram som gjelder menneskelige ressurser, og har opplyst om hvor berørte ansatte kan få tilgang til programmet.

— vil samarbeide med uavhengige klagemekanismer for å kontrollere at organisasjonene faktisk har registrert seg hos den relevante mekanismen angitt i egensertifiseringsmeldingen, dersom slik registrering er nødvendig.

Økt innsats for å følge opp organisasjoner som er blitt fjernet fra Privacy Shield-listen

— underrette organisasjoner som er blitt fjernet fra Privacy Shield-listen på grunn av «vedvarende manglende overholdelse av prinsippene», om at de ikke har rett til å beholde opplysninger samlet inn innenfor rammen av Privacy Shield-ordningen, og

— sende spørreskjemaer til organisasjoner hvis egensertifisering er utløpt eller som frivillig har trukket seg fra Privacy Shield-ordningen, for å kontrollere om organisasjonen akter å sende tilbake, slette eller fortsette å anvende prinsippene på de personopplysningene den mottok mens den deltok i Privacy Shield-ordningen, og, dersom den beholder personopplysningene, kontrollere hvem i organisasjonen som vil fungere som fast kontaktpunkt for spørsmål knyttet til Privacy Shield-ordningen.

Søke etter og håndtere falske påstander om deltakelse

— gjennomgå personvernprogrammet til organisasjoner som tidligere har deltatt i Privacy Shield-ordningen, men som er blitt fjernet fra Privacy Shield-listen, for å avdekke eventuelle falske påstander om deltakelse i Privacy Shield-ordningen,

— løpende, dersom en organisasjon a) trekker seg fra Privacy Shield-programmet, b) ikke foretar en ny sertifisering som bekrefter at den har sluttet seg til prinsippene, eller c) fjernes som deltaker i Privacy Shield-ordningen, særlig på grunn av «vedvarende manglende overholdelse av prinsippene», forplikte seg til *ex officio* å kontrollere at organisasjonen har fjernet enhver henvisning til Privacy Shield-ordningen som antyder at organisasjonen fortsatt deltar aktivt i og har rett til å nyte godt av fordelene ved den, fra alle relevante offentliggjorte personvernprogrammer. Dersom departementet fastslår at nevnte henvisninger ikke er blitt fjernet, vil det advare organisasjonen om at det vil, alt etter hva som er relevant, henvise saken til relevant organ med henblikk på mulige håndhevingstiltak dersom organisasjonen fortsetter å påstå at det er Privacy Shield-sertifisert. Dersom organisasjonen verken fjerner henvisningene eller ved egensertifisering erklærer at den har sluttet seg til Privacy Shield-prinsippene, vil departementet *ex officio* henvise saken til FTC, transportdepartementet eller et annet relevant håndhevingsorgan eller, dersom det er relevant, treffe tiltak for å sikre at Privacy Shield-sertifiseringsmerket respekteres,

— treffe andre tiltak for å avdekke falske påstander om deltakelse i Privacy Shield-ordningen og feilaktig bruk av Privacy Shield-sertifiseringsmerket, herunder ved å foreta søk på internett for å avdekke hvor bilder av Privacy Shield-sertifiseringsmerket vises, samt henvisninger til Privacy Shield-ordningen i organisasjonenes personvernprogrammer,

— reagere raskt på eventuelle problemer vi avdekker i vår *ex officio*-overvåking av falske påstander om deltakelse og feilaktig bruk av sertifiseringsmerket, herunder advare organisasjoner som avgir uriktige opplysninger om sin deltakelse i Privacy Shield-ordningen som beskrevet over,

— treffe andre egnede korrigerende tiltak, herunder ved å bruke de rettsmidlene departementet har til rådighet, og henvise sakene til FTC, transportdepartementet eller et annet relevant rettshåndhevende organ, og

— omgående gjennomgå og behandle klager på falske påstander om deltakelse som vi mottar.

Departementet vil gjennomgå organisasjonenes personvernprogrammer for mer effektivt å kunne avdekke og behandle falske påstander om deltakelse i Privacy Shield-ordningen. Departementet vil særlig gjennomgå personvernprogrammene til organisasjoner hvis egensertifisering er utløpt fordi de ikke har foretatt en ny sertifisering av sin tilslutning til prinsippene. Departementet vil foreta denne typen gjennomgåelser for å kontrollere at disse organisasjonene har fjernet enhver henvisning som antyder at organisasjonen fortsatt deltar aktivt i Privacy Shield-ordningen, fra alle relevante offentliggjorte personvernprogrammer. Slike gjennomgåelser vil føre til at vi kan identifisere organisasjoner som ikke har fjernet slike henvisninger, og disse vil motta et brev fra departementets Office of General Counsel med en advarsel om mulige håndhevingstiltak dersom henvisningene ikke fjernes. Departementet vil treffe oppfølgingstiltak for å sikre at organisasjonene enten fjerner feilaktige henvisninger eller på nytt sertifiserer sin tilslutning til prinsippene. Departementet vil i tillegg treffe tiltak for å avdekke falske påstander om deltakelse i Privacy Shield-ordningen framsatt av organisasjoner som aldri har deltatt i den, og vil treffe lignende korrigerende tiltak overfor slike organisasjoner.

Foreta regelmessige *ex officio*-kontroller og -vurderinger av at ordningen overholdes

— Løpende overvåke at prinsippene faktisk overholdes, herunder ved å sende detaljerte spørreskjemaer til organisasjoner som deltar i ordningen, for å avdekke problemer som kan kreve ytterligere oppfølgingstiltak. Nevnte kontroller skal særlig foretas når a) departementet har mottatt spesifikke og begrunnede klager på en organisasjons manglende overholdelse av prinsippene, b) en organisasjon ikke svarer tilfredsstillende på departementets henvendelser om informasjon knyttet til Privacy Shield-ordningen, eller c) det foreligger troverdig dokumentasjon på at en organisasjon ikke overholder sine forpliktelser i henhold til Privacy Shield-ordningen. Når det er relevant, skal departementet rådføre seg med vedkommende personvernmyndigheter om nevnte kontroller av at prinsippene overholdes.

— Regelmessig vurdere forvaltningen av og tilsynet med Privacy Shield-ordningen for å sikre at overvåkingen er egnet med henblikk på å kunne håndtere nye problemer etter hvert som de oppstår.

Departementet har økt ressursene til forvaltning av og tilsyn med Privacy Shield-ordningen, herunder en dobling av antall medarbeidere med ansvar for forvaltning av og tilsyn med ordningen. Vi vil også framover sette av tilstrekkelige ressurser til dette for å sikre effektivt tilsyn med og forvaltning av programmet.

Skreddersy Privacy Shield-nettstedet til spesielle målgrupper

Departementet vil skreddersy Privacy Shield-nettstedet for tre målgrupper: Privatpersoner og foretak i EU samt foretak i De forente stater. Materiale som er målrettet mot privatpersoner og foretak i EU, vil sikre større åpenhet på en rekke måter. Når det gjelder privatpersoner i EU, vil det bli tydelig forklart 1) hvilke rettigheter Privacy Shield-ordningen gir privatpersoner i EU, 2) hvilke klagemekanismer som er tilgjengelige for privatpersoner i EU når de mener at en organisasjon ikke har oppfylt sin forpliktelse om å overholde prinsippene, og 3) hvor det er mulig å finne informasjon om en organisasjons Privacy Shield-egensertifisering. Når det gjelder foretak i EU, gjøre det lettere å kontrollere 1) om en organisasjon har rett til å nyte godt av fordelene ved Privacy Shield-ordningen, 2) hvilken type informasjon som omfattes av en organisasjons Privacy Shield-egensertifisering, 3) personvernprogrammet som får anvendelse på opplysningene som omfattes, og 4) metoden som organisasjonen bruker for å kontrollere at den overholder prinsippene.

Øke samarbeidet med personvernmyndighetene

For å øke mulighetene for samarbeid med personvernmyndighetene vil departementet utpeke et fast kontaktpunkt som skal ha ansvar for kontakten med personvernmyndighetene. I tilfeller der en personvernmyndighet mener at en organisasjon ikke overholder prinsippene, herunder etter en klage fra en privatperson i EU, kan personvernmyndigheten henvende seg til det faste kontaktpunktet i departementet for å få foretatt en ytterligere kontroll av organisasjonen. Kontaktpunktet vil også få henvist saker som gjelder organisasjoner som feilaktig hevder at de deltar i Privacy Shield-ordningen, selv om de aldri har foretatt egensertifisering og på den måten erklært at de har sluttet seg til prinsippene. Kontaktpunktet vil bistå personvernmyndigheter som søker informasjon om en bestemt organisasjons egensertifisering eller tidligere deltakelse i ordningen, og kontaktpunktet vil svare på personvernmyndighetenes forespørsler om gjennomføringen av særlige Privacy Shield-krav. Departementet vil også gi personvernmyndighetene materiale om Privacy Shield-ordningen som de kan legge ut på sine egne nettsteder, for å øke åpenheten for privatpersoner og foretak i EU. Økt bevissthet om Privacy Shield-ordningen og de rettighetene og pliktene den innebærer, bør gjøre det lettere å identifisere problemer etter hvert som de oppstår, slik at de kan håndteres på egnet måte.

Tiltak for å gjøre det enklere å avgjøre klager på manglende overholdelse av prinsippene

Departementet vil gjennom det faste kontaktpunktet motta klager på at en Privacy Shield-organisasjon ikke overholder prinsippene som det får henvist fra en personvernmyndighet. Departementet vil gjøre sitt ytterste for å avgjøre klagen sammen med Privacy Shield-organisasjonen. Innen 90 dager etter mottak av klagen vil departementet sende en oppdatering om sakens status til personvernmyndigheten. For å gjøre det lettere å inngi slike klager vil departementet utarbeide et standardskjema som personvernmyndighetene kan sende til departementets faste kontaktpunkt. Det faste kontaktpunktet vil spore alle henvisninger som departementet mottar fra personvernmyndighetene, og departementet vil i forbindelse med den årlige gjennomgåelsen beskrevet nedenfor utarbeide en rapport med en analyse i aggregert form av klagene det mottar hvert år.

Innføre voldgiftsprosedyrer og velge voldgiftsmenn i samråd med Kommisjonen

Departementet vil oppfylle sine forpliktelser i vedlegg I og offentliggjøre prosedyrene etter at det er oppnådd enighet.

Felles mekanisme for gjennomgåelse av hvordan Privacy Shield-ordningen fungerer

Det amerikanske handelsdepartementet, FTC og eventuelt andre organer vil avholde årlige møter med Kommisjonen, berørte personvernmyndigheter og relevante representanter for artikkel 29-arbeidsgruppen der departementet vil legge fram oppdatert informasjon om Privacy Shield-ordningen. De årlige møtene vil omfatte drøftinger av aktuelle spørsmål knyttet til gjennomføringen, tilsynet med og håndhevingen av Privacy Shield-ordningen samt hvordan den fungerer, herunder henvisninger som departementet har mottatt fra personvernmyndigheter, og resultatene av *ex officio*-kontrollene av at prinsippene overholdes, og eventuelt drøftinger av relevante lovendringer. Den første årlige gjennomgåelsen og, dersom det er relevant, senere gjennomgåelser vil omfatte en dialog om andre spørsmål, f.eks. om automatiserte avgjørelser, herunder aspekter knyttet til likheter og forskjeller i de metodene som brukes i EU og i De forente stater.

Oppdatering av lovbestemmelser

Departementet vil treffe rimelige tiltak for å underrette Kommisjonen om vesentlige endringer i amerikansk rett, i den grad dette er relevant for Privacy Shield-ordningen med hensyn til vern av personopplysninger samt de begrensningene og garantiene som gjelder for amerikanske myndigheters tilgang til personopplysninger og senere bruk av dem.

Unntak knyttet til nasjonal sikkerhet

Med hensyn til begrensningene som gjelder for tilslutning til Privacy Shield-prinsippene for formål knyttet til nasjonal sikkerhet, har Robert Litt, General Counsel of the Office of the Director of National Intelligence, også sendt to brev til Justin Antonipillai og Ted Dean i handelsdepartementet, og disse er blitt videresendt til dere. Disse brevene inneholder en inngående drøfting av blant annet retningslinjene, garantiene og begrensningene som gjelder for signaletterretningsaktiviteter som utføres av De forente stater. I brevene redegjøres det også for etterretningssamfunnets åpenhet om disse spørsmålene. Ettersom Kommisjonen er i ferd med å vurdere Privacy Shield-ordningen, gir informasjonen i disse brevene nødvendige garantier for å kunne fastslå at Privacy Shield-ordningen vil fungere etter hensikten og i samsvar med prinsippene fastsatt i den. Vi er innforstått med at dere i framtiden kan anvende informasjon som er blitt offentliggjort av etterretningssamfunnet, sammen med annen informasjon, som grunnlag for den årlige gjennomgåelsen av Privacy Shield-ordningen.

På grunnlag av Privacy Shield-prinsippene og vedlagte brev og materiale, herunder departementets forpliktelser med hensyn til forvaltning av og tilsyn med Privacy Shield-ordningen, forventer vi at Kommisjonen vil fastslå at Privacy Shield-avtalen mellom EU og De forente stater gir et tilstrekkelig vern i henhold til EU-retten, og at dataoverføringer fra EU til organisasjoner som deltar i Privacy Shield-ordningen, vil fortsette.

Vennlig hilsen

Ken Hyatt

———

Vedlegg 2

Voldgiftsmodell

VEDLEGG I

I dette vedlegg I angis vilkårene som Privacy Shield-organisasjoner plikter å rette seg etter for å avgjøre klager ved voldgift i henhold til prinsippet om klageadgang, håndheving og ansvar. Muligheten for tvungen voldgift beskrevet nedenfor får anvendelse på visse «resterende» krav vedrørende opplysninger som omfattes av Privacy Shield-avtalen mellom EU og De forente stater. Formålet med dette alternativet er å gi privatpersoner mulighet til å velge en rask, uavhengig og rettferdig mekanisme som kan behandle klager på påståtte overtredelser av prinsippene som ikke er blitt avgjort av eventuelle andre Privacy Shield-mekanismer.

A. **Virkeområde**

En privatperson har i forbindelse med resterende krav mulighet til å bringe saken inn for voldgift for å få fastslått om en Privacy Shield-organisasjon har misligholdt sine forpliktelser overfor vedkommende i henhold til prinsippene, og om det er truffet tiltak for helt eller delvis å korrigere dette. Dette alternativet er tilgjengelig bare for disse formålene. Dette alternativet er f.eks. ikke tilgjengelig i forbindelse med unntakene fra prinsippene([1]) eller når det gjelder påstander om hvorvidt det vernet som Privacy Shield-ordningen sikrer, er tilstrekkelig.

B. **Tilgjengelige rettsmidler**

Denne voldgiftsmuligheten gir Privacy Shield-panelet (som består av en eller tre voldgiftsmenn, avhengig av hva som er avtalt mellom partene) myndighet til å pålegge rimelige individuelle og ikke-økonomiske tiltak (f.eks. innsyn i, retting, sletting eller tilbakesending av vedkommendes opplysninger) som er nødvendige for å korrigere overtredelsen av prinsippene, utelukkende når det gjelder denne privatpersonen. Dette er voldgiftspanelets eneste myndighet når det gjelder rettsmidler. Voldgiftspanelet skal når det vurderer rettslige tiltak, ta høyde for andre rettslige tiltak som allerede er blitt pålagt gjennom andre mekanismer i Privacy Shield-ordningen. Ingen former for skadeserstatning, kostnader, gebyrer eller andre rettsmidler er tilgjengelige. Hver part skal betale sine egne advokatkostnader.

C. **Krav før voldgiftsbehandling**

En privatperson som beslutter å benytte denne voldgiftsmuligheten, skal gjøre følgende før krav framsettes: 1) Ta opp den påståtte overtredelsen direkte med organisasjonen og gi organisasjonen mulighet til å løse problemet innenfor tidsrammen fastsatt i avsnitt III nr. 11 bokstav d) i) i prinsippene, 2) benytte den uavhengige klagemekanismen i henhold til prinsippene, som skal være uten ekstra omkostninger for privatpersonen, og 3) via sin personvernmyndighet legge fram saken for det amerikanske handelsdepartementet og gi det mulighet til å gjøre sitt beste for å løse problemet innenfor tidsrammene fastsatt i brevet fra handelsdepartementets International Trade Administration uten omkostninger for vedkommende.

Det kan ikke framsettes krav om voldgift dersom den samme påståtte overtredelsen av prinsippene i henhold til privatpersonen 1) tidligere har vært gjenstand for tvungen voldgift, 2) har vært gjenstand for en endelig dom avsagt i en rettssak som vedkommende var part i, eller 3) tidligere har vært gjenstand for forlik mellom partene. Denne muligheten kan heller ikke brukes dersom en personvernmyndighet i EU 1) har myndighet i henhold til avsnitt III nr. 5 eller III nr. 9 i prinsippene, eller 2) har myndighet til å avgjøre den påståtte overtredelsen direkte sammen med organisasjonen. En personvernmyndighets myndighet til å avgjøre den samme saken mot en behandlingsansvarlig i EU utelukker ikke alene muligheten til å framsette krav om voldgift overfor et annet rettssubjekt som ikke er bundet av personvernmyndighetens myndighet.

D. **Avgjørelsenes bindende karakter**

En privatperson kan frivillig velge å anvende denne muligheten for tvungen voldgift. Voldgiftsavgjørelser er bindene for alle parter som deltar i voldgiftsprosessen. Når en privatperson har framsatt krav om voldgift, frasier vedkommende seg muligheten til å få samme påståtte overtredelse avgjort i et annet forum. Dersom rimelige ikke-økonomiske tiltak ikke avhjelper den påståtte overtredelsen fullt ut, utelukker det faktum at privatpersonen har framsatt krav om voldgift, imidlertid ikke muligheten til å kreve erstatning ved domstolene.

([1]) Avsnitt I nr. 5 i prinsippene.

E. **Kontroll og håndheving**

Privatpersoner og Privacy Shield-organisasjoner kan anmode om domstolskontroll og håndheving av voldgiftsavgjørelsene i henhold til amerikansk rett, nærmere bestemt Federal Arbitration Act([1]). Slike saker skal bringes inn for vedkommende føderale førsteinstansdomstol der hovedforretningsstedet til Privacy Shield-organisasjonen ligger.

Hensikten med voldgift er å løse individuelle tvister, det er ikke hensikten at voldgiftsavgjørelser skal fungere som overbevisende eller bindende presedens i saker der andre parter er involvert, herunder i framtidige voldgiftssaker for domstoler i EU eller De forente stater eller i FTC-saker.

F. **Voldgiftspanel**

Partene skal velge voldgiftsmenn på listen over voldgiftsmenn omhandlet nedenfor.

I samsvar med gjeldende rett skal det amerikanske handelsdepartementet og Europakommisjonen utarbeide en liste over minst 20 voldgiftsmenn valgt på grunnlag av uavhengighet, integritet og ekspertise. Det følgende får anvendelse i forbindelse med denne prosessen:

Voldgiftsmenn

1) oppføres på listen i en periode på tre år, bortsett fra ved ekstraordinære omstendigheter eller årsaker; denne treårsperioden kan fornyes én gang,

2) skal ikke motta instrukser fra eller være tilknyttet noen part eller noen Privacy Shield-organisasjon eller De forente stater, EU eller EU-medlemsstater eller andre offentlige myndigheter eller håndhevingsmyndigheter, og

3) skal ha rett til å arbeide som advokat i De forente stater og være ekspert på amerikansk personvernlovgivning, og ha ekspertkunnskap om EUs regelverk for vern av personopplysninger.

G. **Voldgiftsprosedyrer**

I henhold til gjeldende rett skal det amerikanske handelsdepartementet og Europakommisjonen innen seks måneder etter vedtakelse av beslutningen om tilstrekkelig beskyttelsesnivå komme til enighet om en rekke eksisterende og veletablerte amerikanske voldgiftsprosedyrer (f.eks. AAA eller JAMS) som skal få anvendelse på saker som bringes inn for Privacy Shield-panelet, idet det tas hensyn til følgende:

1. En privatperson kan innlede sak om tvungen voldgift, forutsatt at ovennevnte krav før voldgift er oppfylt, ved å sende en «melding» til organisasjonen. Meldingen skal inneholde et sammendrag av hva som er gjort i henhold til punkt C for å løse saken, en beskrivelse av den påståtte overtredelsen og – etter vedkommendes valg – eventuelle underlagsdokumenter og -materiale og/eller en analyse av den lovgivningen som får anvendelse på den påståtte overtredelsen.

([1]) I kapittel 2 i Federal Arbitration Act («FAA») fastslås det at «en voldgiftsavtale eller voldgiftskjennelse som følger av et juridisk forhold, avtalefestet eller ikke, som anses som kommersielt, herunder en transaksjon, kontrakt eller avtale beskrevet i [avsnitt 2 i FAA], faller inn under [Convention on the Recognition and Enforcement of Foreign Arbitral Awards av 10. juni 1958, 21 U.S.T. 2519, T.I.A.S. No 6997 («New York-konvensjonen»)].» 9 U.S.C. § 202. I FAA fastslås det videre «at en avtale eller kjennelse som følger av et slikt forhold, og som utelukkende eksisterer mellom amerikanske statsborgere, skal anses for ikke å falle inn under [New York]-konvensjonen, med mindre nevnte forhold omfatter eiendom i utlandet, skal gjennomføres eller håndheves i utlandet eller har en annen rimelig forbindelse til en eller flere fremmede stater.» Id. I henhold til kapittel 2 «kan enhver part i voldgiftssaken anmode enhver domstol med domsmyndighet i henhold til dette kapittel om en kjennelse som bekrefter voldgiftskjennelsen avsagt mot enhver annen part i voldgiftssaken. Domstolen skal bekrefte voldgiftskjennelsen, med mindre den konstaterer at en av grunnene til å nekte eller utsette anerkjennelsen eller fullbyrdelsen av voldgiftskjennelsen angitt i nevnte [New York]-konvensjon foreligger.» Id. § 207. I kapittel 2 fastslås det videre at «distriktsdomstolene i De forente stater … skal ha opprinnelig domsmyndighet over … saker [omfattet av New York-konvensjonen], uansett størrelsen på tvistebeløpet.» Id. § 203.
I kapittel 2 fastslås det også at «kapittel 1 får anvendelse på saker anlagt i henhold til dette kapittel i den grad det aktuelle kapittel ikke er i strid med dette kapittel eller [New York]-konvensjonen som ratifisert av De forente stater.» Id. § 208. I kapittel 1 fastslås det derimot at «en skriftlig bestemmelse i […] en kontrakt om en forretningsmessig transaksjon der en tvist som senere oppstår som følge av denne kontrakten eller transaksjonen eller nektelsen av å oppfylle hele eller deler av denne, skal avgjøres ved voldgift, eller en skriftlig avtale om at en eksisterende tvist oppstått som følge av en slik kontrakt, transaksjon eller nektelse skal avgjøres ved voldgift, er ugyldig, ugjenkallelig og tvangskraftig, med mindre det er andre grunner i henhold til loven eller billighetsprinsippet til å oppheve kontrakter.» Id. § 2. I kapittel 1 fastslås det videre at «enhver part i voldgiftssaken kan anmode vedkommende domstol om en kjennelse som bekrefter voldgiftskjennelsen, og at domstolen deretter skal avsi en slik kjennelse, med mindre voldgiftskjennelsen omstøtes, endres eller rettes som fastsatt i avsnitt 10 og 11 i [FAA].» Id. § 9.

2. Det vil bli utarbeidet prosedyrer for å sikre at den samme påståtte overtredelsen ikke omfattes av flere rettslige tiltak eller prosedyrer.

3. FTC-saker kan anlegges parallelt med voldgiftsbehandlingen.

4. Representanter for De forente stater, EU, EU-medlemsstater eller andre statlige organer, offentlige myndigheter eller håndhevingsmyndigheter kan ikke delta i disse voldgiftsbehandlingene. På anmodning fra en privatperson i EU kan personvernmyndigheter i EU bare bistå med utarbeidingen av meldingen, men kan ikke få tilgang til dokumenter eller annet materiale som gjelder voldgiftsbehandlingen.

5. Voldgiftsbehandlingen vil finne sted i De forente stater, og privatpersonen kan velge å delta via video- eller telefonkonferanse som skal stilles gratis til rådighet for vedkommende. Det er ikke nødvendig å møte opp personlig.

6. Med mindre partene har avtalt noe annet, skal voldgiftsbehandlingen foregå på engelsk. På en begrunnet anmodning og idet det tas hensyn til om privatpersonen representeres av en advokat eller ikke, vil både tolking under voldgiftshøringen og oversettelse av materiale knyttet til voldgiftssaken bli stilt gratis til rådighet for privatpersonen, med mindre panelet vurderer at dette i den aktuelle voldgiftssaken vil føre til uberettigede eller uforholdsmessig høye kostnader.

7. Materiale som legges fram for voldgiftsmenn, vil bli behandlet fortrolig og vil bare bli brukt i forbindelse med voldgiftsbehandlingen.

8. Individuell framlegging av dokumenter kan være tillatt ved behov, og dette vil bli behandlet fortrolig av partene og vil bare bli brukt i forbindelse med voldgiftsbehandlingen.

9. Voldgiftsbehandlingen bør avsluttes senest 90 dager etter at melding er gitt til den berørte organisasjonen, med mindre partene er blitt enige om noe annet.

H. **Kostnader**

Voldgiftsmenn bør treffe rimelige tiltak for å minimere voldgiftskostnadene eller -gebyrene.

Med forbehold for gjeldende rett vil det amerikanske handelsdepartementet i samråd med Europakommisjonen legge til rette for opprettelse av et fond som Privacy Shield-organisasjoner skal betale et årlig bidrag til, som dels er basert på organisasjonens størrelse, og som vil dekke voldgiftskostnadene, herunder honorar til voldgiftsmennene, opp til et maksimumsbeløp («tak»). Fondet vil bli forvaltet av en tredjepart som regelmessig skal rapportere om driften av fondet. Ved den årlige gjennomgåelsen vil det amerikanske handelsdepartementet og Europakommisjonen gjennomgå driften av fondet, herunder om det er behov for å justere bidragsbeløpene eller taket, samt blant annet vurdere antall voldgiftsbehandlinger og kostnadene for og varigheten av disse ut fra en gjensidig forståelse av at Privacy Shield-organisasjoner ikke må pålegges en urimelig stor økonomisk byrde. Advokathonorarer omfattes ikke av denne bestemmelsen eller av eventuelle fond i henhold til denne bestemmelsen.

———

VEDLEGG II

PRINSIPPER I RAMMEVERKET FOR PRIVACY SHIELD-AVTALEN MELLOM EU OG DE FORENTE STATER UTSTEDT AV DET AMERIKANSKE HANDELSDEPARTEMENTET

I. OVERSIKT

1. Både De forente stater og Den europeiske union arbeider for å bedre personvernet, men De forente stater har valgt en annen tilnærming til personvern enn Den europeiske union. I De forente stater anvendes det en sektorvis tilnærming som innebærer en kombinasjon av lovgivning, regulering og selvregulering. På grunn av disse forskjellene og for å gi organisasjoner i De forente stater en pålitelig mekanisme for overføring av personopplysninger fra Den europeiske union til De forente stater og samtidig sikre at registrerte i EU fortsatt nyter godt av effektive garantier og et effektivt vern, noe som er et krav i EUs regelverk for behandling av registrertes personopplysninger når de overføres til tredjestater, har det amerikanske handelsdepartementet i henhold til sin lovfestede myndighet utarbeidet disse Privacy Shield-prinsippene, herunder de supplerende prinsippene (heretter kalt «prinsippene»), for å fremme og utvikle internasjonal handel (15 U.S.C. § 1512). Prinsippene er utarbeidet i samarbeid med Europakommisjonen, næringslivet og andre berørte parter for å fremme handelen mellom De forente stater og Den europeiske union. Prinsippene skal bare anvendes av organisasjoner i De forente stater som mottar personopplysninger fra Den europeiske union, med det formål å oppfylle kravene i Privacy Shield-ordningen og nyte godt av Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå([1]). Prinsippene påvirker ikke anvendelsen av nasjonale bestemmelser som gjennomfører 95/46/EF («direktivet»), og som gjelder behandling av personopplysninger i medlemsstatene. Prinsippene begrenser heller ikke andre forpliktelser på området personvern i henhold til amerikansk rett.

2. For å kunne overføre personopplysninger fra EU innenfor rammen av Privacy Shield-ordningen skal en organisasjon ved egensertifisering ved handelsdepartementet (eller dets representant) («departementet») erklære at den har sluttet seg til prinsippene. Organisasjoner kan fritt velge om de vil delta i Privacy Shield-ordningen, men dersom de deltar, skal prinsippene overholdes: organisasjoner som foretar egensertifisering ved departementet og offentlig erklærer at de har sluttet seg til prinsippene, må overholde prinsippene fullt ut. For å kunne delta i Privacy Shield-ordningen skal en organisasjon a) omfattes av undersøkelses- og håndhevingsmyndigheten til Federal Trade Commission («FTC»), det amerikanske transportdepartementet eller et annet lovfestet organ som vil sikre en effektiv overholdelse av prinsippene *(andre lovfestede amerikanske organer anerkjent av EU kan legges ved som et vedlegg på et senere tidspunkt)*, b) offentlig erklære at den forplikter seg til å overholde prinsippene, c) offentliggjøre sine personvernprogrammer i tråd med disse prinsippene og d) gjennomføre dem fullt ut. En organisasjons manglende overholdelse kan håndheves etter avsnitt 5 i Federal Trade Commission Act som forbyr urimelig og villedende atferd i forbindelse med handel (15 U.S.C. § 45(a)), eller andre lover eller forskrifter som forbyr slik praksis.

3. Det amerikanske handelsdepartementet vil føre og offentliggjøre en offisiell liste over amerikanske organisasjoner som ved egensertifisering ved departementet har forpliktet seg til å overholde prinsippene (heretter kalt «Privacy Shield-listen»). En organisasjon kan nyte godt av Privacy Shield-ordningen fra den datoen da departementet fører opp organisasjonen på Privacy Shield-listen. Departementet vil fjerne en organisasjon fra Privacy Shield-listen dersom organisasjonen trekker seg frivillig fra Privacy Shield-ordningen eller ikke foretar den årlige nye sertifiseringen ved departementet. Dersom en organisasjon fjernes fra Privacy Shield-listen, nyter den ikke lenger godt av Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå i forbindelse med mottak av personopplysninger fra EU. Organisasjonen skal fortsette å anvende prinsippene på de personopplysningene den mottok mens den deltok i Privacy Shield-ordningen, og hvert år bekrefte overfor departementet at den forplikter seg til dette så lenge den er i besittelse av slike opplysninger. I motsatt fall skal organisasjonen sende tilbake eller slette opplysningene eller sørge for et «tilstrekkelig» vern av opplysningene på en annen godkjent måte. Departementet vil også fjerne organisasjoner fra Privacy Shield-listen som over tid har unnlatt å overholde prinsippene. Nevnte organisasjoner har ikke rett til å nyte godt av fordelene ved Privacy Shield-ordningen, og skal sende tilbake eller slette personopplysningene de har mottatt innenfor rammen av Privacy Shield-ordningen.

4. Departementet vil også føre og offentliggjøre en offisiell fortegnelse over amerikanske organisasjoner som tidligere har foretatt egensertifisering ved departementet, men som er blitt fjernet fra Privacy Shield-listen. Departementet vil utstede en tydelig advarsel om at disse organisasjonene ikke deltar i Privacy Shield-ordningen, at organisasjoner som er fjernet fra Privacy Shield-listen, ikke kan hevde at de deltar i Privacy Shield-ordningen og skal unngå enhver uttalelse eller villedende praksis som antyder at de gjør dette, og at slike organisasjoner ikke lenger har rett til å nyte godt av Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå som vil gjøre det mulig for dem å motta personopplysninger fra EU. FTC, transportdepartementet eller andre håndhevingsmyndigheter kan treffe håndhevingstiltak overfor en

([1]) Forutsatt at kommisjonsbeslutningen om tilstrekkelig beskyttelsesnivå som sikres ved Privacy Shield-avtalen mellom EU og De forente stater, får anvendelse på Island, Liechtenstein og Norge, vil Privacy Shield-pakken omfatte både Den europeiske union og disse tre statene. Når det vises til EU og EUs medlemsstater, omfatter dette derfor også Island, Liechtenstein og Norge.

organisasjon som fortsetter å hevde at den deltar i Privacy Shield-ordningen eller avgir andre feilaktige Privacy Shield-relaterte opplysninger etter at den er blitt fjernet fra Privacy Shield-listen.

5. Tilslutningen til disse prinsippene kan være begrenset a) til det som er nødvendig for å oppfylle krav med hensyn til nasjonal sikkerhet, allmennhetens interesse eller rettshåndheving, b) av lover, forskrifter eller rettspraksis som medfører motstridende forpliktelser eller uttrykkelige tillatelser, forutsatt at en organisasjon i forbindelse med anvendelse av slike tillatelser kan dokumentere at dens manglende overholdelse av prinsippene er begrenset til det som er nødvendig for å oppfylle de tungtveiende berettigede interessene som den aktuelle tillatelsen fremmer, eller c) dersom virkningen av direktivet eller medlemsstatenes nasjonale rett er at avvik eller unntak tillates, forutsatt at nevnte avvik eller unntak anvendes i sammenlignbare sammenhenger. I samsvar med målet om å bedre personvernet bør organisasjoner bestrebe seg på å gjennomføre disse prinsippene fullt ut og på en måte som er preget av åpenhet, herunder ved å angi i sine personvernprogrammer der unntak fra prinsippene som er tillatt i henhold til ovennevnte punkt b), får regelmessig anvendelse. Av samme årsak forventes det at organisasjoner velger det høyeste beskyttelsesnivået når dette er mulig, eller når alternativet er tillatt i henhold til prinsippene og/eller amerikansk rett.

6. Organisasjoner plikter å anvende prinsippene på alle personopplysninger som overføres innenfor rammen av Privacy Shield-ordningen, etter at de har sluttet seg til Privacy Shield-ordningen. En organisasjon som velger å utvide Privacy Shield-fordelene til å omfatte personopplysninger om menneskelige ressurser som overføres fra EU med henblikk på bruk i forbindelse med et arbeidsforhold, må opplyse om dette når den foretar egensertifisering ved departementet, og oppfylle kravene fastsatt i det supplerende prinsippet om egensertifisering.

7. Amerikansk rett får anvendelse på fortolkningen og overholdelsen av prinsippene samt relevante Privacy Shield-organisasjoners personvernprogrammer, bortsett fra når disse organisasjonene har forpliktet seg til å samarbeide med europeiske personvernmyndigheter. Med mindre annet er fastsatt, får alle bestemmelsene i prinsippene anvendelse når det er relevant.

8. Definisjoner:

   a. Med «personopplysninger» menes opplysninger om en identifisert eller identifiserbar privatperson som hører inn under direktivets virkeområde, mottatt av en organisasjon i De forente stater fra Den europeiske union og registrert på en hvilken som helst måte.

   b. Med «behandling» av personopplysninger menes enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering eller spredning samt sletting eller tilintetgjøring.

   c. Med «behandlingsansvarlig» menes en person eller en organisasjon som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

9. Prinsippene får anvendelse på datoen for den endelige godkjenningen av Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå.

II. PRINSIPPER

1. **Opplysningsplikt**

   a. En organisasjon skal underrette registrerte om

      i. at den deltar i Privacy Shield-ordningen og angi en lenke, eller nettadressen, til Privacy Shield-listen,

      ii. typer innsamlede personopplysninger og, dersom det er relevant, organisasjonens enheter eller datterforetak som også har sluttet seg til prinsippene,

iii. at den har forpliktet seg til å anvende prinsippene på alle personopplysninger som mottas fra EU innenfor rammen av Privacy Shield-ordningen,

iv. hvilke formål som ligger til grunn for innsamlingen og bruken av personopplysninger som gjelder dem,

v. hvordan organisasjonen kan kontaktes ved spørsmål eller klager, herunder relevante organer i EU som kan svare på nevnte spørsmål eller klager,

vi. hvilken type eller identiteten til tredjeparter som den utleverer personopplysninger til, og formålet med dette,

vii. privatpersoners rett til å få innsyn i egne personopplysninger,

viii. valgmulighetene og midlene som organisasjonen tilbyr privatpersoner for å begrense bruken og utleveringen av deres personopplysninger,

ix. det uavhengige tvisteløsningsorganet som er utpekt for å behandle klager og sikre egnet gratis klageadgang for privatpersoner, og om det er 1) panelet opprettet av personvernmyndighetene, 2) et alternativt tvisteløsningsorgan basert i EU eller 3) et alternativt tvisteløsningsorgan basert i De forente stater,

x. at den er underlagt undersøkelses- og håndhevingsmyndigheten gitt FTC, det amerikanske transportdepartementet eller andre amerikanske offisielle organer,

xi. privatpersonens mulighet for på visse vilkår å kreve tvungen voldgift,

xii. kravet om å utlevere personopplysninger som svar på offentlige myndigheters lovlige anmodninger, herunder for å oppfylle krav knyttet til nasjonal sikkerhet eller rettshåndheving, og

xiii. sitt ansvar ved videreoverføringer til tredjeparter.

b. Opplysningene skal formidles på et klart og enkelt språk første gang privatpersoner blir bedt om å gi personopplysninger til organisasjonen, eller så raskt som mulig deretter, men i alle tilfeller før organisasjonen bruker nevnte opplysninger for et annet formål enn det de opprinnelig ble samlet inn eller behandlet for av organisasjonen som har overført opplysningene, eller før de utleveres for første gang til en tredjepart.

2. **Valgmulighet**

a. En organisasjon skal gi privatpersoner mulighet til å velge om deres personopplysninger i) skal utleveres til en tredjepart eller ii) brukes for et formål som er vesentlig forskjellig fra formålet/formålene de opprinnelig ble samlet inn for, eller formål som privatpersonene senere har godkjent. Privatpersoner skal på en tydelig og lett tilgjengelig måte gis mulighet til å utøve denne valgmuligheten.

b. Som unntak fra forrige punkt er det ikke nødvendig å tilby valgmulighet når opplysningene utleveres til en tredjepart som fungerer som representant og utfører oppgaver på vegne av og på instruks fra organisasjonen. En organisasjon skal imidlertid alltid inngå en avtale med representanten.

c. Når det gjelder sensitive opplysninger (dvs. personopplysninger om helsetilstand, rasemessig eller etnisk opprinnelse, politisk oppfatning, religion eller filosofisk overbevisning, fagforeningsmedlemskap eller opplysninger om privatpersonens seksuelle legning), skal organisasjoner innhente privatpersonenes uttrykkelige samtykke dersom slike opplysninger skal i) utleveres til en tredjepart eller ii) brukes for et annet formål enn det de opprinnelig ble samlet inn for, eller formål som privatpersonene senere har godkjent. En organisasjon skal i tillegg behandle alle personopplysninger som den mottar fra en tredjepart, som sensitive når tredjeparten identifiserer og behandler dem som sensitive.

3. **Ansvar for videreoverføring**

a. For å overføre personopplysninger til en tredjepart som opptrer som behandlingsansvarlig, må organisasjoner overholde prinsippene om opplysningsplikt og valgmulighet. Organisasjonene må også inngå en avtale med den behandlingsansvarlige tredjeparten der det fastsettes at nevnte opplysninger bare kan behandles for begrensede og spesifikke formål som er i samsvar med privatpersonens samtykke, og at mottakeren vil sikre det samme beskyttelsesnivået som det som sikres i prinsippene, og underrette organisasjonen dersom den fastslår at den ikke lenger kan oppfylle denne forpliktelsen. Det skal framgå av avtalen at når dette fastslås, skal tredjeparten som opptrer som behandlingsansvarlig, avslutte behandlingen eller treffe andre rimelige og egnede korrigerende tiltak.

b. For å overføre personopplysninger til en tredjepart som opptrer som representant, skal organisasjoner i) overføre nevnte opplysninger bare for begrensede og spesifikke formål, ii) bekrefte at representanten plikter å sikre minst samme nivå for vern av personopplysninger som det som kreves i prinsippene, iii) treffe rimelige og egnede tiltak for å sikre at representanten faktisk behandler de overførte personopplysningene på en måte som er i samsvar med organisasjonens forpliktelser i henhold til prinsippene, iv) kreve at representanten underretter organisasjonen dersom den fastslår at den ikke lenger kan oppfylle plikten til å sikre det samme beskyttelsesnivået som det som kreves i prinsippene, v) etter underretning, herunder i henhold til punkt iv), treffe rimelige og egnede tiltak for å innstille og korrigere uautorisert behandling og vi) legge fram et sammendrag eller en representativ kopi av de relevante personvernbestemmelsene i avtalen med nevnte representant for departementet på anmodning.

4. **Sikkerhet**

a. Organisasjoner som oppretter, forvalter, bruker eller sprer personopplysninger, skal treffe rimelige og egnede tiltak for å verne opplysningene mot tap, misbruk og uautorisert tilgang, utlevering, endring og tilintetgjøring, idet det tas behørig hensyn til de risikoene som behandlingen innebærer, samt personopplysningenes art.

5. **Dataintegritet og formålsbegrensning**

a. I henhold til prinsippene skal personopplysninger være begrenset til opplysninger som er relevante for formålet med behandlingen([1]). En organisasjon kan ikke behandle personopplysninger på en måte som er uforenlig med de formålene de ble samlet inn for, eller formål som privatpersonen senere har godkjent. En organisasjon skal i den grad det er nødvendig for disse formålene, treffe rimelige tiltak for å sikre at personopplysningene er pålitelige for den planlagte bruken, samt at de er riktige, fullstendige og oppdaterte. En organisasjon skal overholde prinsippene så lenge den er i besittelse av nevnte opplysninger.

b. Opplysningene kan oppbevares på en måte som identifiserer privatpersonen eller gjør vedkommende identifiserbar([2]), bare så lenge de tjener et behandlingsformål i henhold til punkt 5a. Denne plikten hindrer ikke organisasjoner i å behandle personopplysninger i lengre perioder så lenge og i den grad nevnte behandling med rimelighet tjener arkivformål i allmennhetens interesse og formål knyttet til journalistikk, litteratur og kunst, vitenskapelig og historisk forskning samt statistisk analyse. I disse tilfellene skal slik behandling omfattes av de andre prinsippene og bestemmelsene i ordningen. Organisasjoner bør treffe rimelige og egnede tiltak for å oppfylle denne bestemmelsen.

6. **Innsyn**

a. Privatpersoner skal ha rett til å få innsyn i personopplysninger som gjelder dem, og som en organisasjon er i besittelse av, og skal ha mulighet til å rette, endre eller slette opplysninger dersom de er uriktige eller er blitt behandlet i strid med prinsippene, bortsett fra dersom arbeidet eller kostnadene ved å gi innsyn vil være uforholdsmessig store i forhold til risikoene for privatpersonens personvern, eller dersom det medfører at andre privatpersoners rettigheter blir krenket.

([1]) Alt etter omstendighetene kan eksempler på forenlige behandlingsformål omfatte formål som med rimelighet tjener kunderelasjoner, formål som gjelder overholdelse og juridiske hensyn, revisjon, sikkerhet og bedrageriforebygging, opprettholdelse eller beskyttelse av organisasjonens juridiske rettigheter eller andre formål som er i samsvar med en forstandig persons forventninger ut fra sammenhengen innsamlingen utføres i.

([2]) I denne forbindelse anses en privatperson for å være «identifiserbar» dersom vedkommende på bakgrunn av den med rimelighet forventede identifikasjonsmetoden (idet det bl.a. tas hensyn til kostnadene for og tiden som er nødvendig for identifisering, og den tilgjengelige teknologien på tidspunktet for behandlingen) og måten opplysningene oppbevares på, med rimelighet kan identifiseres av organisasjonen eller en tredjepart dersom denne har tilgang til opplysningene.

7. **Klageadgang, håndheving og ansvar**

a. Et effektivt vern av personopplysninger skal omfatte robuste mekanismer for å sikre at prinsippene overholdes, klageadgang for privatpersoner som påvirkes av manglende overholdelse av prinsippene, og konsekvenser for organisasjonen dersom den ikke følger prinsippene. Nevnte mekanismer skal som et minimum omfatte

i. lett tilgjengelige og uavhengige klagemekanismer som gjør det mulig å undersøke klager og tvister og raskt avgjøre dem uten ekstra omkostninger for privatpersonen og ved henvisning til prinsippene, og å gi skadeserstatning når dette er fastsatt i gjeldende rett eller i initiativer innen den private sektor,

ii. oppfølgingsprosedyrer for å kontrollere at de forsikringene og bekreftelsene som organisasjoner avgir om sin personvernpraksis, er riktige, og at nevnte praksis er blitt gjennomført som beskrevet, særlig når det gjelder tilfeller av manglende overholdelse, og

iii. en plikt til å korrigere problemer som skyldes at organisasjoner som har erklært at de følger prinsippene, ikke overholder disse, samt konsekvenser for nevnte organisasjoner. Sanksjonene må være tilstrekkelig strenge til å sikre at organisasjonene overholder prinsippene.

b. Organisasjoner og deres utvalgte uavhengige klagemekanismer skal omgående besvare henvendelser og forespørsler fra departementet om informasjon knyttet til Privacy Shield-ordningen. Alle organisasjoner skal svare raskt på klager på manglende overholdelse av prinsippene som EU-medlemsstatenes myndigheter henviser via departementet. Organisasjoner som har valgt å samarbeide med personvernmyndigheter, herunder organisasjoner som behandler opplysninger om menneskelige ressurser, skal svare direkte til nevnte myndigheter når det gjelder undersøkelser og avgjørelser av klager.

c. Organisasjoner plikter å avgjøre klager ved voldgift og overholde vilkårene i vedlegg I dersom privatpersonen har krevd å få klagen avgjort ved tvungen voldgift ved å sende en melding til den berørte organisasjonen, og etter framgangsmåtene og på de vilkårene som er omhandlet i vedlegg I.

d. I forbindelse med videreoverføring har en Privacy Shield-organisasjon ansvar for behandlingen av de personopplysningene den mottar innenfor rammen av Privacy Shield-ordningen, og deretter overfører til en tredjepart som opptrer som representant på dens vegne. Privacy Shield-organisasjonen skal fortsatt være ansvarlig i henhold til prinsippene dersom dens representant behandler nevnte personopplysninger i strid med prinsippene, med mindre organisasjonen beviser at den ikke er ansvarlig for hendelsen som forvoldte skaden.

e. Dersom en organisasjon blir gjenstand for en avgjørelse fra FTC eller en rettsavgjørelse på grunn av manglende overholdelse, skal organisasjonen offentliggjøre alle relevante Privacy Shield-relaterte avsnitt i alle overholdelses- eller vurderingsrapporter som legges fram for FTC, i den grad dette er forenlig med kravene til fortrolighet. Departementet har opprettet et fast kontaktpunkt som personvernmyndigheter kan henvende seg til dersom Privacy Shield-organisasjoner ikke overholder prinsippene. FTC vil prioritere henviste saker om manglende overholdelse av prinsippene fra departementet og EU-medlemsstatenes myndigheter, og vil i rett tid utveksle informasjon om slike saker med henvisende statlige myndigheter, med forbehold for gjeldende begrensninger med hensyn til fortrolighet.

III. SUPPLERENDE PRINSIPPER

1. **Sensitive opplysninger**

a. En organisasjon plikter ikke å innhente et uttrykkelig samtykke i forbindelse med sensitive opplysninger dersom behandlingen

i. er nødvendig for å verne den registrertes eller en annen persons vitale interesser,

ii. er nødvendig for å fastslå eller forsvare et rettslig krav,

iii. kreves i forbindelse med medisinsk behandling eller diagnostisering,

iv. utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, filosofisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter, forutsatt at behandlingen bare gjelder organets medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til en tredjepart uten de registrertes samtykke,

v. er nødvendig for å oppfylle organisasjonens forpliktelser på det arbeidsrettslige området, eller

vi. gjelder personopplysninger som det er åpenbart at privatpersonen har offentliggjort.

2. **Unntak for journalistiske formål**

a. På bakgrunn av vernet fastsatt i den amerikanske grunnloven med tanke på pressefrihet, samt direktivets unntak for journalistisk materiale, skal det, når prinsippet om pressefrihet nedfelt i første tillegg til den amerikanske grunnloven kommer i konflikt med personvernet, foretas en avveining av disse interessene i henhold til første grunnlovstillegg når det dreier seg om amerikanske personers eller organisasjoners virksomhet.

b. Personopplysninger som samles inn med tanke på offentliggjøring, kringkasting eller andre former for offentlig formidling av journalistisk materiale, enten det blir brukt eller ikke, samt opplysninger fra tidligere offentliggjort materiale som spres fra pressearkiver, er ikke underlagt Privacy Shield-prinsippene.

3. **Sekundært ansvar**

a. Internettleverandører, teleselskaper og andre organisasjoner er ikke ansvarlige i henhold til Privacy Shield-prinsippene når de på vegne av en annen organisasjon utelukkende overfører, ruter, svitsjer eller lagrer opplysninger. Verken direktivet eller Privacy Shield-ordningen gir grunnlag for sekundært ansvar. Når en organisasjon fungerer utelukkende som kanal for opplysninger som overføres av tredjeparter, og ikke fastsetter formålene med eller metodene for behandling av nevnte personopplysninger, kan organisasjonen ikke holdes ansvarlig.

4. **Gjennomføring av selskapsgjennomgåelser og revisjoner**

a. Investeringsbankers og revisorers virksomhet kan omfatte behandling av personopplysninger uten at privatpersonen er blitt underrettet eller har gitt sitt samtykke. Dette er tillatt i henhold til prinsippene om opplysningsplikt, valgmulighet og innsyn i situasjonene beskrevet nedenfor.

b. Offentlige aksjeselskaper og fåmannsselskaper, herunder Privacy Shield-organisasjoner, er regelmessig gjenstand for revisjoner. Slike revisjoner, særlig revisjoner der det ses nærmere på eventuelle uregelmessigheter, kan settes på spill dersom de offentliggjøres for tidlig. En Privacy Shield-organisasjon som er involvert i en potensiell fusjon eller overtakelse, skal også foreta eller være gjenstand for en selskapsgjennomgåelse («due diligence»). Dette vil ofte innebære innsamling og behandling av personopplysninger, f.eks. opplysninger om den øverste ledelsen og annet nøkkelpersonell. En for tidlig offentliggjøring kan hindre transaksjonen eller til og med være i strid med gjeldende verdipapirbestemmelser. Investeringsbanker og advokater som er involvert i selskapsgjennomgåelser, eller revisorer som foretar revisjoner, kan behandle personopplysninger uten at privatpersonen vet det, bare i den grad og i det tidsrommet som er nødvendig for å oppfylle lovfestede krav eller ivareta viktige samfunnsinteresser, samt under andre omstendigheter der anvendelse av nevnte prinsipper vil skade organisasjonens berettigede interesser. Disse berettigede interessene omfatter overvåking av at organisasjoner overholder sine rettslige forpliktelser og berettigede regnskapsplikt, og behovet for fortrolighet i forbindelse med mulige overtakelser, fusjoner, fellesforetak eller lignende transaksjoner som utføres av investeringsbanker eller revisorer.

5. **Personvernmyndighetenes rolle**

a. Organisasjoner skal oppfylle sin plikt til å samarbeide med Den europeiske unions personvernmyndigheter som beskrevet nedenfor. I henhold til Privacy Shield-ordningen skal amerikanske organisasjoner som mottar person-opplysninger fra EU, forplikte seg til å innføre effektive mekanismer for å sikre overholdelse av Privacy Shield-prinsippene. Nærmere bestemt skal deltakende organisasjoner som fastsatt i prinsippet om klageadgang, håndheving og ansvar sørge for bokstav a) i) klageadgang for privatpersonene, bokstav a) ii) oppfølgingsprosedyrer for å kontrollere at de forsikringene og bekreftelsene organisasjonene gir om sin personvernpraksis, er riktige og bokstav a) iii) plikt til å rette opp problemer som skyldes manglende overholdelse av prinsippene, samt konsekvenser for slike organisasjoner. En organisasjon kan oppfylle bokstav a) i) og a) iii) i prinsippet om klageadgang, håndheving og ansvar dersom den oppfyller de kravene om samarbeid med personvernmyndighetene som angis der.

b. En organisasjon plikter å samarbeide med personvernmyndighetene ved at den i sin Privacy Shield-egensertifisering til det amerikanske handelsdepartementet (se det supplerende prinsippet om egensertifisering) bekrefter at den

i. akter å oppfylle kravene i bokstav a) i) og a) iii) i Privacy Shield-prinsippet om klageadgang, håndheving og ansvar ved å forplikte seg til å samarbeide med personvernmyndighetene,

ii. vil samarbeide med personvernmyndighetene om å undersøke og avgjøre klager som mottas innenfor rammen av Privacy Shield-ordningen, og

iii. vil følge eventuelle anbefalinger fra personvernmyndighetene når de mener at organisasjonen må treffe særlige tiltak for å overholde Privacy Shield-prinsippene, herunder utbedringstiltak eller betaling av erstatning til privatpersoner som er blitt berørt av den manglende overholdelsen av prinsippene, og bekrefte skriftlig overfor personvernmyndighetene at nevnte tiltak er truffet.

c. Panel av personvernmyndigheter

i. Personvernmyndighetenes samarbeid skjer i form av informasjon og anbefalinger på følgende måte:

1. Anbefalinger fra personvernmyndighetene vil bli formidlet gjennom et uformelt panel av personvern-myndigheter opprettet på unionsplan som blant annet vil bidra til en enhetlig og sammenhengende tilnærming.

2. Panelet vil gi anbefalinger til berørte amerikanske organisasjoner med hensyn til uløste klager fra privatpersoner på behandling av personopplysninger som er blitt overført fra EU innenfor rammen av Privacy Shield-ordningen. Disse anbefalingene skal være av en slik art at de sikrer at Privacy Shield-prinsippene anvendes riktig, og skal omfatte opplysninger om hvilke rettsmidler de berørte privatpersonene kan gjøre gjeldende, og som personvernmyndighetene anser som hensiktsmessige.

3. Panelet vil utstede slike anbefalinger når det får henvist en sak fra berørte organisasjoner og/eller mottar klager direkte fra privatpersoner på organisasjoner som har forpliktet seg til å samarbeide med personvernmyndighetene innenfor rammen av Privacy Shield-ordningen, og det vil oppfordre og om nødvendig bistå disse privatpersonene med i første omgang å bruke de interne klagebehandlingsordningene som vedkommende organisasjon tilbyr.

4. Anbefalinger vil bli utstedt først etter at begge parter i en tvist har hatt rimelig anledning til å komme med merknader og legge fram eventuelle bevis som de finner relevant. Panelet vil bestrebe seg på å utstede anbefalingene så raskt som dette kravet om behørig behandling tillater. Normalt vil panelet utstede sine anbefalinger senest 60 dager etter mottak av en klage eller henvisning, om mulig enda raskere.

5. Dersom panelet finner det formålstjenlig, vil det offentliggjøre resultatene av behandlingen av de mottatte klagene.

6. Verken panelet eller de enkelte personvernmyndighetene kan holdes ansvarlig for panelets anbefalinger.

ii. Som angitt ovenfor, plikter organisasjoner som velger denne typen tvisteløsning, å etterkomme personvern-myndighetenes anbefalinger. Dersom en organisasjon ikke har etterkommet anbefalingen innen 25 dager etter at den ble gitt, og ikke har gitt en tilfredsstillende forklaring på årsaken til dette, vil panelet meddele at det enten akter å henvise saken til Federal Trade Commission, transportdepartementet eller et annet amerikansk føderalt organ eller delstatsorgan med lovfestet myndighet til å treffe håndhevingstiltak ved villedende praksis og uriktige opplysninger, eller fastslå at det foreligger et alvorlig brudd på samarbeidsavtalen, som dermed skal anses som ugyldig. I sistnevnte tilfelle vil panelet underrette handelsdepartementet slik at Privacy Shield-listen kan endres tilsvarende. Ethvert mislighold av forpliktelsen til å samarbeide med personvernmyndighetene og enhver manglende overholdelse av Privacy Shield-prinsippene kan forfølges rettslig som villedende praksis i henhold til avsnitt 5 i Federal Trade Commission Act eller tilsvarende lovgivning.

d. En organisasjon som ønsker at Privacy Shield-fordelene skal omfatte opplysninger om menneskelige ressurser som overføres fra EU i forbindelse med et arbeidsforhold, må forplikte seg til å samarbeide med personvernmyndighetene i forbindelse med nevnte opplysninger (se det supplerende prinsippet om opplysninger om menneskelige ressurser).

e. Organisasjoner som velger dette alternativet, vil bli avkrevd en årsavgift som skal dekke panelets driftskostnader, og de kan i tillegg bli bedt om å dekke eventuelle kostnader for oversettelse som følge av panelets behandling av henviste saker eller klager på organisasjonene. Årsavgiften skal være på høyst 500 USD og vil være lavere for mindre bedrifter.

6. **Egensertifisering**

a. Organisasjoner nyter godt av fordelene ved Privacy Shield-ordningen fra den datoen da departementet fører opp organisasjonen på Privacy Shield-listen etter å ha fastslått at den avgitte egensertifiseringsmeldingen er fullstendig.

b. En organisasjon kan slutte seg til Privacy Shield-ordningen ved egensertifisering ved å sende en egensertifiseringsmelding til departementet som skal være undertegnet av en ledende medarbeider på vegne av organisasjonen, og som skal inneholde minst følgende opplysninger:

i. Organisasjonens navn, postadresse, e-postadresse, telefon- og faksnummer.

ii. En beskrivelse av organisasjonens virksomhet med hensyn til personopplysninger som mottas fra EU.

iii. En beskrivelse av organisasjonens personvernprogram for slike personopplysninger, herunder

1. dersom organisasjonen har et offentlig nettsted, nettadressen der personvernprogrammet er tilgjengelig, eller dersom organisasjonen ikke har et offentlig nettsted, hvor allmennheten kan få tilgang til personvernprogrammet,

2. ikrafttredelsesdatoen,

3. en kontaktadresse for behandling av klager, anmodninger om innsyn og eventuelle andre Privacy Shield-relaterte spørsmål,

4. det spesifikke lovfestede organet med myndighet til å behandle klager på organisasjonen som gjelder urimelig eller villedende praksis eller brudd på personvernlover og -forskrifter (og som er angitt i prinsippene eller i et framtidig vedlegg til prinsippene),

5. navnet på eventuelle personvernprogrammer som organisasjonen deltar i,

6. kontrollmetoder (f.eks. internkontroll, kontroll foretatt av en tredjepart) (se det supplerende prinsippet om kontroll) og

7. den uavhengige klagemekanismen for behandling av uløste klager.

c. Dersom en organisasjon ønsker at Privacy Shield-fordelene også skal omfatte opplysninger om menneskelige ressurser overført fra EU til bruk i forbindelse med et arbeidsforhold, kan dette tillates dersom et av de lovfestede organene angitt i prinsippene eller i et framtidig vedlegg til prinsippene har myndighet til å behandle klager på organisasjonen som gjelder behandling av opplysninger om menneskelige ressurser. I tillegg må organisasjonen angi dette i egensertifiseringsmeldingen og erklære at den forplikter seg til å samarbeide med den eller de berørte EU-myndighetene i samsvar med de supplerende prinsippene om opplysninger om menneskelige ressurser og personvernmyndighetenes rolle, samt at den akter å følge nevnte myndigheters anbefalinger. Organisasjonen skal også legge fram en kopi av sitt personvernprogram som gjelder menneskelige ressurser, for departementet samt opplyse om hvor berørte ansatte kan få tilgang til personvernprogrammet.

d. Departementet vil opprette Privacy Shield-listen over alle organisasjoner som har inngitt fullstendige egensertifiseringsmeldinger, slik at de kan nyte godt av Privacy Shield-fordelene, og vil oppdatere listen på grunnlag av årlige nye egensertifiseringsmeldinger og meldinger mottatt i henhold til det supplerende prinsippet om tvisteløsning og håndheving. Slike egensertifiseringsmeldinger må minst inngis årlig, og dersom dette ikke gjøres, fjernes organisasjonen fra Privacy Shield-listen og vil ikke lenger kunne nyte godt av Privacy Shield-fordelene. Både Privacy Shield-listen og organisasjonenes egensertifiseringsmeldinger vil bli offentliggjort. Alle organisasjoner som departementet oppfører på Privacy Shield-listen, skal i sine relevante offentliggjorte personvernprogrammer også angi

at de følger Privacy Shield-prinsippene. Dersom en organisasjons personvernprogram er tilgjengelig på nettet, skal det inneholde en hyperlenke til departementets Privacy Shield-nettsted samt en hyperlenke til klageskjemaet for eller nettstedet til den uavhengige klagemekanismen med ansvar for å behandle uløste klager.

e. Personvernprinsippene får anvendelse umiddelbart etter sertifisering. Prinsippene vil få innvirkning på handelsforbindelser med tredjeparter, og organisasjoner som sertifiserer sin tilslutning til Privacy Shield-ordningen i de to første månedene etter at den er iverksatt, skal bringe eksisterende handelsforbindelser med tredjeparter i samsvar med prinsippet om ansvar for videreoverføring så snart som mulig, og i alle tilfeller senest ni måneder etter datoen for sertifisering av organisasjonens deltakelse i Privacy Shield-ordningen. Når organisasjoner i denne overgangsperioden overfører opplysninger til en tredjepart, skal de i) anvende prinsippene om opplysningsplikt og valgmulighet og ii) dersom personopplysninger overføres til en tredjepart som opptrer som representant, bekrefte at representanten plikter å sørge for minst samme beskyttelsesnivå som det som kreves i prinsippene.

f. En organisasjon skal anvende Privacy Shield-prinsippene på alle personopplysninger som mottas fra EU innenfor rammen av Privacy Shield-ordningen. Forpliktelsen til å følge Privacy Shield-prinsippene er ikke tidsbegrenset for personopplysninger som mottas i det tidsrommet organisasjonen nyter godt av fordelene ved Privacy Shield-ordningen. Forpliktelsen innebærer at organisasjonen må fortsette å anvende prinsippene på slike opplysninger så lenge den lagrer, bruker eller utleverer dem, selv om organisasjonen av en eller annen grunn senere skulle forlate Privacy Shield-ordningen. En organisasjon som trekker seg fra Privacy Shield-ordningen, men som ønsker å beholde slike opplysninger, skal årlig bekrefte overfor departementet at den vil fortsette å anvende prinsippene eller sørge for et «tilstrekkelig» vern av opplysningene på en annen godkjent måte (f.eks. ved å bruke en avtale som fullt ut gjenspeiler kravene i de relevante standardavtalevilkårene vedtatt av Europakommisjonen). Dersom dette ikke er tilfellet, skal organisasjonen sende tilbake eller slette opplysningene. En organisasjon som trekker seg fra Privacy Shield-ordningen, skal fjerne enhver henvisning som antyder at organisasjonen fortsatt deltar aktivt i og har rett til å nyte godt av fordelene ved den, fra alle relevante offentliggjorte personvernprogrammer.

g. En organisasjon som som følge av fusjon eller overtakelse vil opphøre som eget rettssubjekt, må melde dette på forhånd til departementet. I meldingen skal det også angis om den enheten som overtar, eller den enheten som oppstår ved fusjonen, i) fortsatt vil være bundet av Privacy Shield-prinsippene i henhold til de lovbestemmelsene som gjelder for overtakelsen eller fusjonen, eller ii) ved egensertifisering velger å slutte seg til Privacy Shield-prinsippene eller treffer andre sikkerhetstiltak, f.eks. en skriftlig avtale som sikrer at Privacy Shield-prinsippene overholdes. Dersom verken i) eller ii) får anvendelse, skal alle personopplysninger mottatt innenfor rammen av Privacy Shield-ordningen slettes med det samme.

h. Dersom en organisasjon av en eller annen grunn trer ut av Privacy Shield-ordningen, skal den fjerne alle erklæringer som antyder at den fortsatt deltar i eller har rett til å nyte godt av fordelene ved den. Dersom Privacy Shield-sertifiseringsmerket brukes, skal også det fjernes. En organisasjon som gir uriktige opplysninger til allmennheten om at den har sluttet seg til Privacy Shield-prinsippene, kan bringes inn for FTC eller et annet relevant offentlig organ. Uriktige opplysninger til departementet kan medføre rettslig forfølging i henhold til False Statements Act (18 U.S.C. § 1001).

7. **Kontroll**

a. Organisasjonene skal ha oppfølgingsprosedyrer for å kontrollere at de forsikringene og bekreftelsene de gir om sin personvernpraksis innenfor rammen av Privacy Shield-ordningen, er riktige, og at nevnte praksis er blitt gjennomført som beskrevet i samsvar med Privacy Shield-prinsippene.

b. For å oppfylle kravet om kontroll i prinsippet om klageadgang, håndheving og ansvar skal en organisasjon kontrollere nevnte forsikringer og bekreftelser enten gjennom egenvurdering eller ekstern kontroll av overholdelsen.

c. Ved egenvurdering skal det kontrolleres om organisasjonens offentliggjorte personvernprogram for personopplysninger mottatt fra EU er riktig, dekkende, om det i tilstrekkelig grad er blitt offentliggjort, er fullt ut gjennomført og tilgjengelig. Det må også framgå at personvernprogrammet er i samsvar med Privacy Shield-prinsippene, at privatpersoner blir underrettet om eventuelle interne ordninger for behandling av klager samt om uavhengige klagemekanismer, at det finnes prosedyrer for å gi ansatte opplæring i hvordan de skal gjennomføre programmet og for å gripe inn dersom programmet ikke følges, samt at organisasjonen har interne prosedyrer for regelmessig og objektiv kontroll av at det ovenstående overholdes. En ledende medarbeider eller en annen representant med fullmakt

i organisasjonen skal minst én gang i året undertegne en erklæring om at det er foretatt egenvurdering, og denne erklæringen skal gjøres tilgjengelig på anmodning fra privatpersoner eller i forbindelse med en undersøkelse eller klage på manglende overholdelse.

d. Dersom en organisasjon velger ekstern kontroll av overholdelsen, skal kontrollen påvise at organisasjonens personvernprogram for personopplysninger mottatt fra EU, er i samsvar med Privacy Shield-prinsippene, at programmet følges, og at privatpersoner blir underrettet om klagemekanismer. Kontrollmetodene kan uten begrensning omfatte revisjon, stikkprøver, bruk av falske opplysninger som «lokkemat» eller andre teknologiske verktøyer som måtte passe. Kontrolløren, en ledende medarbeider eller en annen representant i organisasjonen med fullmakt skal minst én gang i året undertegne en erklæring om at det er foretatt ekstern kontroll av overholdelsen, og denne erklæringen skal gjøres tilgjengelig på anmodning fra privatpersoner eller i forbindelse med en undersøkelse eller klage på manglende overholdelse.

e. Organisasjoner skal dokumentere iverksettingen av sin personvernpraksis innenfor rammen av Privacy Shield-ordningen, og på anmodning, i forbindelse med undersøkelser eller klager på manglende overholdelse, gjøre slik dokumentasjon tilgjengelig for det uavhengige organet med ansvar for å undersøke klager eller for den instansen som har ansvar for saker om urimelig eller villedende praksis. Organisasjoner skal også omgående besvare henvendelser og andre anmodninger om informasjon fra departementet knyttet til organisasjonens tilslutning til prinsippene.

8. **Innsyn**

a. Innsynsprinsippet i praksis

i. I henhold til Privacy Shield-prinsippene er retten til innsyn av avgjørende betydning for personvernet. Den gir privatpersoner mulighet til å kontrollere at opplysningene om dem er riktige. Prinsippet om innsyn innebærer at registrerte har rett til å

1. få opplyst om en organisasjon behandler personopplysninger om dem eller ikke([1]),

2. få utlevert nevnte opplysninger, slik at de kan kontrollere at de er riktige og at behandlingen er lovlig, og

3. få opplysningene rettet, endret eller slettet dersom de er uriktige eller behandles i strid med prinsippene.

ii. En privatperson trenger ikke å begrunne en anmodning om innsyn i opplysninger om seg selv. Organisasjoner som mottar anmodninger om innsyn, bør først og fremst la seg styre av hva som ligger til grunn for anmodningen. Dersom en anmodning om innsyn f.eks. er vag eller for omfattende, kan organisasjonen innlede en dialog med privatpersonen for bedre å forstå bakgrunnen for anmodningen og dermed lettere finne de relevante opplysningene. Organisasjonen kan spørre om hvilken del eller hvilke deler av organisasjonen vedkommende har vært i kontakt med, eller hvilken type opplysninger eller bruk anmodningen om innsyn gjelder.

iii. I henhold til innsynsprinsippet skal organisasjoner alltid utvise velvilje med hensyn til å gi innsyn. Dersom for eksempel visse opplysninger må beskyttes og lett kan skilles fra andre personopplysninger som det anmodes om innsyn i, skal organisasjonen redigere bort de beskyttede opplysningene og gi innsyn i de øvrige. Dersom organisasjonen i særlige tilfeller beslutter at innsynet bør begrenses, skal den begrunne avgjørelsen overfor den privatpersonen som har anmodet om innsyn, og opplyse om hvor vedkommende kan henvende seg for nærmere opplysninger.

b. Arbeidsbyrde eller kostnader ved å gi innsyn

i. Retten til innsyn i personopplysninger kan begrenses i særlige tilfeller der det vil medføre en krenkelse av andre personers berettigede interesser, eller der arbeidsbyrden eller kostnadene ved å gi innsyn vil være uforholdsmessig store i forhold til risikoene for privatpersonens personvern i det aktuelle tilfellet. Kostnader og arbeidsbyrde er viktige faktorer som det må tas hensyn til, men de er ikke avgjørende for om det er rimelig å gi innsyn.

([1]) Organisasjonen bør svare på en privatpersons anmodninger om formålene med behandlingen, hvilke kategorier av personopplysninger som er berørt, og mottakerne eller kategoriene av mottakere som personopplysningene utleveres til.

ii. Dersom for eksempel personopplysningene danner grunnlag for avgjørelser som er av vesentlig betydning for den enkelte (f.eks. avslag på eller tildeling av viktige ytelser som forsikring og lån eller ansettelse), skal organisasjonen i samsvar med de øvrige bestemmelsene i disse supplerende prinsippene gi innsyn i slike opplysninger, selv om dette er relativt vanskelig eller medfører høye kostnader. Dersom personopplysningene det anmodes om, ikke er sensitive eller ikke danner grunnlag for avgjørelser som i vesentlig grad vil påvirke den enkelte, men er lett tilgjengelige og med få omkostninger kan gjøres tilgjengelige, skal en organisasjon gi innsyn i slike opplysninger.

c. Fortrolige forretningsopplysninger

i. Fortrolige forretningsopplysninger er opplysninger som en organisasjon har beskyttet mot offentliggjøring, fordi offentliggjøring vil være fordelaktig for en konkurrent i markedet. En organisasjon kan nekte eller begrense innsyn dersom den ved å gi fullt innsyn risikerer å avsløre egne fortrolige forretningsopplysninger, f.eks. markedsføringskonsepter og klassifiseringer den har utarbeidet, eller andres fortrolige forretningsopplysninger som i henhold til en avtaleforpliktelse skal behandles fortrolig.

ii. Dersom forretningsopplysninger lett kan skilles fra andre personopplysninger som det anmodes om innsyn i, skal organisasjonen redigere bort de fortrolige forretningsopplysningene og gi innsyn i de øvrige.

d. Organisering av databaser

i. En organisasjon kan gi innsyn ved å utlevere de relevante personopplysningene til privatpersonen, og dette krever ikke at privatpersonen gis tilgang til organisasjonens database.

ii. En organisasjon skal gi innsyn bare i den grad organisasjonen lagrer personopplysningene. Innsynsprinsippet innebærer ikke en plikt til å oppbevare, forvalte, omorganisere eller omstrukturere personopplysningsregistre.

e. Begrenset innsyn

i. Ettersom organisasjoner alltid skal utvise velvilje med hensyn til å gi privatpersoner innsyn i egne personopplysninger, kan de bare begrense nevnte innsyn i begrensede tilfeller, og enhver slik begrensning skal begrunnes. På samme måte som i henhold til direktivet kan en organisasjon nekte å gi innsyn i opplysninger dersom dette antas å vanskeliggjøre vern av viktige offentlige interesser, f.eks. nasjonal sikkerhet, forsvar eller offentlig sikkerhet. I tillegg kan innsyn nektes når personopplysninger behandles utelukkende for statistiske formål eller forskningsformål. Innsyn kan også nektes eller begrenses i tilfeller der det

1. vanskeliggjør gjennomføring eller håndheving av loven eller sivile søksmål, herunder forebygging, etterforskning eller avsløring av lovovertredelser eller retten til en rettferdig rettergang,

2. medfører en krenkelse av andre personers berettigede rettigheter eller viktige interesser,

3. er et brudd på lovfestede eller andre yrkesmessige rettigheter eller plikter,

4. vanskeliggjør sikkerhetsundersøkelser av arbeidstakere eller behandling av klager eller i forbindelse med personalplanlegging eller omstrukturering, eller

5. reduserer fortroligheten som er nødvendig i forbindelse med overvåking, inspeksjon eller reguleringsfunksjoner forbundet med god forvaltning, eller framtidige eller løpende forhandlinger som organisasjonen er involvert i.

ii. En organisasjon som påberoper seg et unntak, skal dokumentere at nevnte unntak er nødvendig, begrunne avgjørelsen om begrenset innsyn og opplyse om hvor de registrerte kan henvende seg ved behov for ytterligere opplysninger.

f. Rett til å motta bekreftelse og rett til å kreve et gebyr for å dekke kostnadene forbundet med å gi innsyn

i. En person har rett til å få opplyst om en organisasjon innehar personopplysninger om ham eller henne. En person har også rett til å få utlevert sine personopplysninger. En organisasjon kan kreve et rimelig gebyr.

ii. Det kan være berettiget å kreve et gebyr, f.eks. dersom anmodninger om innsyn er tydelig overdrevne, særlig fordi de gjentas.

iii. Dersom privatpersonen tilbyr seg å dekke kostnadene, kan innsyn ikke nektes av kostnadshensyn.

g. Gjentatte eller useriøse anmodninger om innsyn

En organisasjonen kan fastsette en passende grense for hvor mange ganger de vil behandle anmodninger om innsyn fra en bestemt person innenfor et gitt tidsrom. Når de fastsetter slike grenser, må organisasjonene ta hensyn til faktorer som hvor ofte opplysningene oppdateres, for hvilket formål de brukes, og opplysningenes art.

h. Bedragerske anmodninger om innsyn

En organisasjon er ikke forpliktet til å gi innsyn, med mindre den mottar tilstrekkelig informasjon som gjør det mulig å bekrefte identiteten til personen som framsetter anmodningen.

i. Svarfrist

Organisasjoner bør svare på anmodninger om innsyn innen en rimelig frist, på en rimelig måte og i et format som er lettfattelig for den enkelte. En organisasjon som regelmessig utleverer opplysninger til registrerte, kan besvare en individuell anmodning om innsyn innenfor rammen av sin regelmessige utlevering av opplysninger dersom det ikke medfører en urimelig forsinkelse.

9. **Opplysninger om menneskelige ressurser**

a. Privacy Shield-ordningens omfang

i. Dersom en organisasjon i EU overfører personopplysninger om sine ansatte (nåværende eller tidligere) som er samlet inn i forbindelse med arbeidsforholdet, til en tjenesteyter i USA, det være seg et morselskap, et tilknyttet eller ikke-tilknyttet foretak, som deltar i Privacy Shield-ordningen, omfattes overføringen av Privacy Shield-ordningen. I slike tilfeller skal innsamlingen og behandlingen av opplysningene før overføring være i samsvar med nasjonal lovgivning i den EU-staten der opplysningene ble samlet inn, og alle vilkår eller begrensninger for overføring i henhold til nevnte lovgivning skal overholdes.

ii. Privacy Shield-prinsippene er relevante bare ved overføring av eller innsyn i individuelt identifiserte eller identifiserbare opplysninger. Statistiske rapporter som bygger på aggregerte ansettelsesopplysninger, og som ikke inneholder personopplysninger eller anonymiserte opplysninger, utgjør ikke en risiko for personvernet.

b. Anvendelse av prinsippene om opplysningsplikt og valgmulighet

i. En amerikansk organisasjon som har mottatt ansatteopplysninger fra EU innenfor rammen av Privacy Shield-ordningen, kan utlevere dem til tredjeparter eller bruke dem for forskjellige formål bare dersom det skjer i samsvar med prinsippene om opplysningsplikt og valgmulighet. Dersom en amerikansk organisasjon for eksempel akter å bruke personopplysninger som er samlet inn i forbindelse med et arbeidsforhold, til formål som ikke gjelder arbeidsforholdet, f.eks. markedsføring, må organisasjonen først gi de berørte privatpersonene en mulighet til å velge, med mindre de allerede har samtykket i en slik bruk av opplysningene. En slik bruk må ikke være uforenlig med formålene som personopplysningene er blitt samlet inn for, eller formål som privatpersonen senere har godkjent. De ansattes valg må heller ikke føre til at deres karrieremuligheter begrenses eller til at det iverksettes straffetiltak mot dem.

ii. Det bør bemerkes at visse vilkår som får alminnelig anvendelse på overføringer fra visse medlemsstater i EU, kan utelukke annen bruk av slike opplysninger, selv etter overføring til land utenfor EU, og at slike vilkår skal overholdes.

iii. I tillegg skal arbeidsgivere bestrebe seg på å oppfylle arbeidstakerens ønsker når det gjelder personvern. Dette kan for eksempel innebære at det gis begrenset innsyn i personopplysninger, at visse opplysninger anonymiseres, eller at det brukes koder eller pseudonymer dersom de virkelige navnene ikke er nødvendige for formålet med opplysningene.

iv. En organisasjon er ikke forpliktet til å anvende prinsippene om opplysningsplikt og valgmulighet i den grad og i det tidsrommet som er nødvendig for ikke å skade organisasjonens interesser i forbindelse med forfremmelser, utnevnelser eller lignende personalsaker.

c. Anvendelse av innsynsprinsippet

Det supplerende prinsippet om innsyn inneholder en veiledning om årsaker til å nekte innsyn eller gi begrenset innsyn i opplysninger om menneskelige ressurser. Arbeidsgivere i EU må naturligvis overholde nasjonale bestemmelser og sørge for å sikre at arbeidstakere i EU har tilgang til slike opplysninger i samsvar med lovgivningen i sine hjemstater, uansett hvor opplysningene behandles eller lagres. Privacy Shield-ordningen forutsetter at en organisasjon som behandler slike opplysninger i USA, vil samarbeide for å gi innsyn enten direkte eller gjennom arbeidsgiveren i EU.

d. Håndheving

i. Såframt personopplysningene anvendes bare innenfor rammen av arbeidsforholdet, er det organisasjonen i EU om har hovedansvaret for opplysningene overfor arbeidstakeren. Det vil si at når europeiske arbeidstakere klager på at deres personvernrettigheter er krenket, og ikke er tilfreds med utfallet av prosedyrene for internkontroll, klage eller anke (eller en hvilken som helst annen klageprosedyre etter avtale med en fagforening), bør de henvises til vedkommende nasjonale personvern- eller sysselsettingsmyndighet der de arbeider. Dette omfatter også saker der ansvaret for den påståtte feilbehandlingen av personopplysningene ligger hos den amerikanske organisasjonen som har mottatt opplysningene fra arbeidsgiveren, og dermed omfatter et påstått brudd på Privacy Shield-prinsippene. Dette vil være den mest effektive framgangsmåten for å håndtere de ofte overlappende rettighetene og forpliktelsene som er fastsatt i nasjonal arbeidsrett og arbeidsavtaler samt i personvernlovgivninger.

ii. En amerikansk organisasjon som deltar i Privacy Shield-ordningen, og som bruker opplysninger om menneskelige ressurser overført fra EU innenfor rammen av et arbeidsforhold, og som ønsker at slike overføringer skal omfattes av Privacy Shield-ordningen, må derfor i slike tilfeller forplikte seg til å samarbeide ved undersøkelser som foretas av vedkommende EU-myndigheter, og følge deres anbefalinger.

e. Anvendelse av prinsippet om ansvar for videreoverføring

I forbindelse med leilighetsvise arbeidsforholdsrelaterte behov i Privacy Shield-organisasjonen som gjelder personopplysninger overført innenfor rammen av Privacy Shield-ordningen, f.eks. bestilling av flybilletter, hotellrom eller forsikringsdekning, kan personopplysninger om et lite antall ansatte overføres til behandlingsansvarlige uten anvendelse av innsynsprinsippet eller inngåelse av en avtale med den behandlingsansvarlige tredjeparten, noe som ellers er et krav i henhold til prinsippet om ansvar for videreoverføring, forutsatt at Privacy Shield-organisasjonen har overholdt prinsippene om opplysningsplikt og valgmulighet.

10. **Obligatoriske avtaler om videreoverføringer**

a. Avtaler om behandling av personopplysninger

i. Når personopplysninger overføres fra EU til De forente stater utelukkende for behandlingsformål, skal det inngås en avtale, uavhengig av om databehandleren deltar i Privacy Shield-ordningen eller ikke.

ii. Behandlingsansvarlige i EU skal alltid inngå en avtale når opplysninger overføres utelukkende for behandling, uansett om behandlingen foregår innenfor eller utenfor EU, og uavhengig av om databehandlere deltar i Privacy Shield-ordningen eller ikke. Formålet med avtalen er å sikre at databehandleren

1. bare opptrer på instruks fra den behandlingsansvarlige,

2. treffer nødvendige tekniske og organisatoriske tiltak for å verne personopplysninger mot utilsiktet eller ulovlig tilintetgjøring eller utilsiktet tap, endring, uautorisert utlevering eller tilgang samt vet om videreoverføring er tillatt eller ikke, og

3. tar hensyn til behandlingens art og bistår den behandlingsansvarlige med å svare på anmodninger fra privatpersoner som utøver sine rettigheter i henhold til prinsippene.

iii. Ettersom deltakerne i Privacy Shield-ordningen sørger for et tilstrekkelig vern, kreves det ikke forhåndsgodkjenning av avtaler med slike deltakere som utelukkende gjelder behandling av opplysninger (eller EU-medlemsstatene vil gi slik godkjenning automatisk), slik det kreves for avtaler med mottakere som ikke deltar i Privacy Shield-ordningen, eller som på annet vis ikke sørger for et tilstrekkelig vern.

b. Overføringer i en kontrollert gruppe av selskaper eller enheter

Når personopplysninger overføres mellom to behandlingsansvarlige i en kontrollert gruppe av selskaper eller enheter, er det ikke alltid nødvendig å inngå en avtale i henhold til prinsippet om ansvar for videreoverføring. Behandlingsanvarlige i en kontrollert gruppe av selskaper eller enheter kan basere slike overføringer på andre instrumenter, f.eks. bindende virksomhetsregler i EU eller andre konserninterne instrumenter (f.eks. overholdelses- og kontrollprogrammer), som vil sikre kontinuitet i vernet av personopplysninger i henhold til prinsippene. I forbindelse med slike overføringer er det Privacy Shield-organisasjonene som fortsatt har ansvar for at prinsippene overholdes.

c. Overføringer mellom behandlingsansvarlige

I forbindelse med overføringer mellom behandlingsansvarlige trenger den mottakende behandlingsansvarlige ikke å være en Privacy Shield-organisasjon eller ha en uavhengig klagemekanisme. Privacy Shield-organisasjonen skal inngå en avtale med den mottakende behandlingsansvarlige tredjeparten som sikrer det samme beskyttelsesnivået som det som sikres i Privacy Shield-ordning, men uten kravet om at den behandlingsansvarlige tredjeparten skal være en Privacy Shield-organisasjon eller ha en uavhengig klagemekanisme, forutsatt at den stiller til rådighet en tilsvarende mekanisme.

11. **Tvisteløsning og håndheving**

a. I prinsippet om klageadgang, håndheving og ansvar er det fastsatt hvordan Privacy Shield-ordningen skal håndheves. I det supplerende prinsippet om kontroll er det fastsatt hvordan kravene i prinsippets bokstav a) ii) skal overholdes. Dette supplerende prinsippet omhandler bokstav a) i) og a) iii), der det stilles krav til uavhengige klagemekanismer. Nevnte mekanismer kan være av ulik art, men de må oppfylle kravene i prinsippet om klageadgang, håndheving og ansvar. Organisasjoner kan oppfylle kravene på følgende måter: i) Ved å overholde personvernprogrammer utarbeidet i privat sektor der Privacy Shield-prinsippene er innlemmet, og som omfatter effektive håndhevingsmekanismer av den typen som er beskrevet i prinsippet om klageadgang, håndheving og ansvar, ii) ved å underkaste seg de tilsynsmyndigheter opprettet ved lov eller administrativt som tar hånd om behandling av individuelle klager og tvisteløsning, eller iii) ved å forplikte seg til å samarbeide med personvernmyndigheter i EU eller deres godkjente representanter.

b. Denne listen er veiledende og ikke fullstendig. Den private sektor kan innføre andre håndhevingsmekanismer, såframt kravene i prinsippet om klageadgang, håndheving og ansvar samt de supplerende prinsippene oppfylles. Det bør bemerkes at kravene i prinsippet om klageadgang, håndheving og ansvar kommer i tillegg til kravet om at

selvregulering skal kunne håndheves etter avsnitt 5 i Federal Trade Commission Act, som forbyr urimelig eller villedende atferd, eller en annen lov eller forskrift som forbyr nevnte praksis.

c. For å bidra til å sikre overholdelse av forpliktelsene i henhold til Privacy Shield-ordningen og for å lette forvaltningen av ordningen skal organisasjoner og deres uavhengige klagemekanismer legge fram informasjon knyttet til Privacy Shield-ordningen når departementet anmoder om det. Organisasjoner skal i tillegg svare raskt på klager på manglende overholdelse av prinsippene som personvernmyndighetene henviser via departementet. Svaret skal inneholde en vurdering av hvorvidt klagen er berettiget, og, dersom dette er tilfellet, opplysninger om hvordan organisasjonen vil korrigere problemet. Departementet vil sørge for at opplysninger det mottar i samsvar med amerikansk rett, behandles fortrolig.

d. Klagemekanismer

i. Forbrukere skal oppfordres til å rette eventuelle klager til den berørte organisasjonen før de henvender seg til uavhengige klagemekanismer. Organisasjoner skal svare på henvendelser fra forbrukere innen 45 dager etter å ha mottatt en klage. Hvorvidt en klagemekanisme er uavhengig, kjennetegnes f.eks. av at den er upartisk, at det er åpenhet om hvordan den er sammensatt og finansieres, og at det foreligger dokumentert erfaring. Som fastsatt i prinsippet om klageadgang, håndheving og ansvar skal klagemekanismen være lett tilgjengelig og gratis for privatpersoner. Tvisteløsningsorganer skal undersøke hver klage som mottas fra privatpersoner, med mindre klagene er åpenbart grunnløse eller useriøse. Dette utelukker ikke at organisasjoner som har opprettet klagemekanismen, innfører kriterier for hvilke klager som kan behandles, men slike kriterier må være begrunnede og preget av åpenhet (f.eks. kriterier for å utelukke klager som faller utenfor ordningens virkeområde, eller som bør behandles i et annet forum) og skal ikke føre til at plikten til å undersøke berettigede klager undermineres. I tillegg bør klagemekanismene gi privatpersoner som inngir en klage, fullstendig og lett tilgjengelig informasjon om hvordan tvisteløsningsprosedyren fungerer. Slik informasjon skal omfatte en beskrivelse av mekanismens personvernpraksis i samsvar med Privacy Shield-prinsippene. De bør også delta i samarbeidet om å utvikle hjelpemidler, f.eks. standardiserte klageskjemaer, som skal gjøre det lettere å avgjøre klagen.

ii. Uavhengige klagemekanismer skal på sine offentlige nettsteder informere om Privacy Shield-prinsippene og tjenestene de tilbyr innenfor rammen av Privacy Shield-ordningen. Disse opplysningene skal omfatte 1) informasjon om eller en lenke til kravene om uavhengige klagemekanismer innenfor rammen av Privacy Shield-prinsippene, 2) en lenke til departementets Privacy Shield-nettsted, 3) informasjon om at deres tvisteløsningstjenester knyttet til Privacy Shield-ordningen er gratis for privatpersoner, 4) en beskrivelse av hvordan en Privacy Shield-relatert klage kan inngis, 5) informasjon om tidsrammen for behandling av Privacy Shield-relaterte klager og 6) en beskrivelse av forskjellige potensielle rettsmidler.

iii. Uavhengige klagemekanismer skal hvert år offentliggjøre en årlig rapport med aggregert statistikk over sine tvisteløsningstjenester. Den årlige rapporten skal inneholde 1) informasjon om det samlede antallet Privacy Shield-relaterte klager som er mottatt i rapporteringsåret, 2) typen klager som er mottatt, 3) kvalitetsindikatorer for tvisteløsning, f.eks. klagebehandlingstid, og 4) utfallet av de mottatte klagene, særlig antall og typer pålagte korrigerende tiltak eller sanksjoner.

iv. Som angitt i vedlegg I har en privatperson i forbindelse med resterende krav mulighet til å bringe saken inn for voldgift for å få fastslått om en Privacy Shield-organisasjon har misligholdt sine forpliktelser overfor vedkommende i henhold til prinsippene, og om det er truffet tiltak for helt eller delvis å korrigere dette. Dette alternativet er tilgjengelig bare for disse formålene. Dette alternativet er f.eks. ikke tilgjengelig i forbindelse med unntakene fra prinsippene([1]) eller når det gjelder påstander om hvorvidt det vernet som Privacy Shield-ordningen sikrer, er tilstrekkelig. Denne voldgiftsmuligheten gir Privacy Shield-panelet (som består av en eller tre voldgiftsmenn, avhengig av hva som er avtalt mellom partene) myndighet til å pålegge rimelige individuelle og ikke-økonomiske tiltak (f.eks. innsyn i, retting, sletting eller tilbakesending av vedkommendes opplysninger) som er nødvendige for å korrigere overtredelsen av prinsippene, utelukkende når det gjelder denne privatpersonen. Privatpersoner og Privacy Shield-organisasjoner kan anmode om domstolskontroll og håndheving av voldgiftsavgjørelsene i henhold til amerikansk rett, nærmere bestemt Federal Arbitration Act.

([1]) Avsnitt I nr. 5 i prinsippene.

e. Rettsmidler og sanksjoner

De rettsmidlene som tvisteløsningsorganet stiller til rådighet, bør føre til at organisasjonen så langt det lar seg gjøre, opphever eller korrigerer følgene av den manglende overholdelsen, og at organisasjonens framtidige behandling av opplysninger skjer i samsvar med prinsippene, samt eventuelt at behandlingen av personopplysninger om vedkommende som har framsatt klagen, innstilles. Sanksjonene skal være tilstrekkelig strenge til å sikre at organisasjonen overholder prinsippene. En rekke sanksjoner av ulik strenghetsgrad vil gi tvisteløsningsorganene mulighet til å reagere på egnet måte på ulike grader av manglende overholdelse. Slike sanksjoner bør omfatte både offentliggjøring av manglende overholdelse og krav om å slette opplysninger i visse tilfeller([1]). Andre mulige sanksjoner kan omfatte midlertidig oppheving eller tilbaketrekking av en godkjenning, erstatning til privatpersoner for tap som følge av manglende overholdelse og forbud. Organer for tvisteløsning og selvregulering i den private sektor skal underrette vedkommende offentlige organ med myndighet eller domstolene om Privacy Shield-organisasjoner som ikke retter seg etter deres avgjørelser, samt underrette departementet.

f. Tiltak fra Federal Trade Commission (FTC)

FTC har forpliktet seg til først og fremst å behandle saker om påstått manglende overholdelse av prinsippene som det får henvist fra i) selvreguleringsorganisasjoner på personvernområdet eller andre uavhengige tvisteløsningsorganer, ii) EU-medlemsstatene og iii) departementet, for å fastslå om det foreligger brudd på avsnitt 5 i FTC Act som forbyr urimelig og villedende atferd eller praksis innenfor handel. Dersom FTC kommer til at det sannsynligvis foreligger brudd på avsnitt 5, kan saken løses ved å søke å oppnå et administrativt forbud mot den aktuelle praksisen eller ved å klage til en føderal førsteinstansdomstol, som kan resultere i en føderal rettsavgjørelse med samme virkning dersom klageren får medhold. Dette omfatter falske påstander om tilslutning til Privacy Shield-prinsippene eller deltakelse i Privacy Shield-ordningen framsatt av organisasjoner som ikke lenger er oppført på Privacy Shield-listen, eller som aldri har foretatt egensertifisering ved departementet. FTC kan oppnå sivilrettslige sanksjoner ved overtredelse av et administrativt forbud mot fortsatt virksomhet, og kan innlede sivilrettslige eller strafferettslige saker ved unnlatelse av å etterkomme føderale rettsavgjørelser. FTC vil underrette departementet om alle slike tiltak. Departementet oppfordrer andre offentlige organer til å underrette departementet om den endelige avgjørelsen i slike saker, eller andre avgjørelser om hvorvidt Privacy Shield-prinsippene overholdes.

g. Vedvarende manglende overholdelse av prinsippene

i. Dersom en organisasjon gjentatte ganger unnlater å overholde prinsippene, har den ikke lenger rett til å nyte godt av fordelene ved Privacy Shield-ordningen. Organisasjoner som over tid har unnlatt å overholde prinsippene, vil bli fjernet fra Privacy Shield-listen av departementet og skal sende tilbake eller slette personopplysningene de har mottatt innenfor rammen av Privacy Shield-ordningen.

ii. Vedvarende manglende overholdelse av prinsippene foreligger når en organisasjon som har foretatt egen-sertifisering ved departementet, nekter å etterkomme den endelige avgjørelsen fra et selvreguleringsorgan, uavhengig tvisteløsningsorgan eller et offentlig organ på personvernområdet, eller når et slikt organ fastslår at en organisasjon overtrer prinsippene så ofte at den ikke lenger er troverdig når den påstår at den gjør det. I slike tilfeller skal organisasjonen umiddelbart underrette departementet om dette. Dersom organisasjonen unnlater å gjøre dette, kan det gi grunnlag for rettslig forfølgning i henhold til False Statements Act (18 U.S.C. § 1001). En organisasjon som trekker seg fra et selvreguleringsprogram på personvernområdet i den private sektor eller fra en uavhengig tvisteløsningsmekanisme, må fremdeles overholde prinsippene. Dersom dette ikke er tilfellet, vil det bli ansett som en vedvarende manglende overholdelse av prinsippene.

iii. Departementet vil fjerne en organisasjon fra Privacy Shield List-listen som reaksjon på meldinger det mottar om gjentatte overtredelser, uansett om de er mottatt fra organisasjonen selv, et selvreguleringsorgan eller et annet uavhengig tvisteløsningsorgan på personvernområdet eller fra et offentlig organ, men først etter å ha gitt

([1]) Tvisteløsningsorganer kan anvende slike sanksjoner etter eget skjønn. Ved vurdering av krav om at opplysninger skal slettes, skal det tas i betraktning hvor sensitive de aktuelle opplysningene er, og om organisasjonen har samlet inn, brukt eller utlevert opplysninger på en måte som åpenbart er i strid med Privacy Shield-prinsippene.

vedkommende organisasjon en frist på 30 dager og mulighet til å svare. Det vil altså klart framgå av Privacy Shield-listen som forvaltes av departementet, hvilke organisasjoner som er anerkjent som «Privacy Shield»-organisasjoner, og hvilke som ikke lenger er det.

iv. En organisasjon som søker om å bli underlagt et selvreguleringsorgan for på nytt å kvalifisere for Privacy Shield-ordningen, må gi nevnte organ all informasjon om sin tidligere deltakelse i Privacy Shield-ordning.

12. **Valgmulighet – tidsfrister for å reservere seg**

a. Formålet med prinsippet om valgmulighet er generelt å sikre at personopplysninger brukes og utleveres i samsvar med den enkeltes forventninger og ønsker. Derfor skal privatpersoner til enhver tid ha mulighet til å reservere seg mot at personopplysninger om dem brukes i direkte markedsføring, innenfor rimelige tidsfrister som organisasjonen fastsetter, f.eks. for at organisasjonen skal få tid til å iverksette den enkeltes valg. En organisasjon kan også kreve tilstrekkelig informasjon for å kunne fastslå identiteten til den privatpersonen som ønsker å reservere seg. I De forente stater kan privatpersoner utøve denne valgmuligheten gjennom et sentralt program for dette formål, f.eks. Direct Marketing Association's Mail Preference Service. Organisasjoner som deltar i Direct Marketing Association's Mail Preference Service, skal opplyse forbrukere som ikke ønsker å motta reklame, om denne tjenesten. Under alle omstendigheter skal en privatperson gis mulighet til på en lett tilgjengelig og økonomisk overkommelig måte å utøve denne valgmuligheten.

b. En organisasjon kan også bruke opplysninger til visse direkte markedsføringsformål når det i praksis ikke er mulig å gi privatpersonen muligheten til å reservere seg før opplysningene brukes, dersom organisasjonen samtidig (og når som helst, på anmodning) gir privatpersonen mulighet (uten ekstra omkostninger) til å reservere seg mot å motta ytterligere direkte markedsføring, og dersom organisasjonen retter seg etter privatpersonens ønsker.

13. **Reiseopplysninger**

a. Opplysninger om plassreservasjon for flypassasjerer og andre reiseopplysninger, f.eks. opplysninger om passasjerer som flyr ofte («frequent flyer»), hotellbestillinger eller om særlige behov, f.eks. måltider tilberedt etter visse religiøse retningslinjer eller fysisk assistanse, kan overføres til organisasjoner utenfor EU i flere forskjellige situasjoner. I henhold til direktivets artikkel 26 kan personopplysninger overføres «til en tredjestat som ikke sikrer et tilstrekkelig vernenivå i henhold til artikkel 25 nr. 2» dersom i) det er nødvendig for å kunne yte de tjenestene kunden ber om, eller for å oppfylle vilkårene i en avtale, f.eks. en avtale for passasjerer som flyr ofte, eller ii) dersom kunden har gitt sitt uttrykkelige samtykke til det. Amerikanske organisasjoner som deltar i Privacy Shield-ordningen, sikrer et tilstrekkelig vern av personopplysninger og kan derfor motta opplysninger fra EU uten å oppfylle disse vilkårene eller andre vilkår i direktivets artikkel 26. Ettersom Privacy Shield-ordningen inneholder særlige regler for sensitive opplysninger, skal slike opplysninger (f.eks. om en passasjerers behov for fysisk assistanse) inngå i opplysninger som overføres til deltakere i Privacy Shield-ordningen. Likevel må organisasjonen som overfører opplysningene, under alle omstendigheter følge lovgivningen i den EU-medlemsstaten der den utøver sin virksomhet, noe som bl.a. kan medføre særlige vilkår for behandling av sensitive opplysninger.

14. **Legemidler**

a. <u>Anvendelse av EU-medlemsstatenes nasjonale rett eller Privacy Shield-prinsippene</u>

EU-medlemsstatenes nasjonale rett får anvendelse på innsamling av personopplysninger og på all behandling som finner sted før opplysningene overføres til De forente stater. Privacy Shield-prinsippene får anvendelse først etter at opplysningene er blitt overført til De forente stater. Opplysninger som brukes i forbindelse med legemiddelforskning og andre formål, bør om nødvendig anonymiseres.

b. Framtidig vitenskapelig forskning

i. Personopplysninger som framkommer gjennom spesifikk medisinsk forskning eller legemiddelforskning, er ofte viktig for framtidig vitenskapelig forskning. Når personopplysninger som er samlet inn i forbindelse med en forskningsstudie, overføres til en amerikansk organisasjon innenfor rammen av Privacy Shield-ordningen, kan denne organisasjonen bruke opplysningene til ny vitenskapelig forskning dersom prinsippene om opplysningsplikt og valgmulighet ble fulgt fra begynnelsen. En eventuell framtidig spesifikk bruk av opplysningene, f.eks. regelmessig oppfølging, beslektede studier eller markedsføring, skal framgå av meldingen som gis i henhold til prinsippet om opplysningsplikt.

ii. Det er ikke mulig å opplyse om all framtidig bruk av opplysningene, ettersom ny innsikt i opprinnelige opplysninger, nye medisinske oppdagelser og framskritt samt utvikling innenfor folkehelse og lovgivning kan føre til ny bruk av forskningen. I meldingen skal det derfor eventuelt opplyses om at personopplysningene kan bli brukt i framtidig medisinsk og farmasøytisk forskningsvirksomhet som det ikke er mulig å forutse. Dersom slik bruk ikke er i samsvar med de alminnelige forskningsformålene som opplysningene opprinnelig ble samlet inn for, eller formål som privatpersonen senere har samtykket i, må det innhentes nytt samtykke.

c. Mulighet til å trekke seg fra en klinisk utprøving

Deltakere kan når som helst selv bestemme seg for eller bli oppfordret til å trekke seg fra en klinisk utprøving. Alle personopplysninger som er blitt innsamlet før deltakerne trekker seg, kan fortsatt behandles på samme måte som andre opplysninger som samles inn i forbindelse med den kliniske utprøvingen, men bare dersom deltakeren ble opplyst om dette da vedkommende samtykket i å delta.

d. Overføringer for formål knyttet til regulering og kontroll

Selskaper som framstiller legemidler eller medisinsk utstyr, har med henblikk på regulering og kontroll lov til å formidle personopplysninger fra kliniske utprøvinger utført i EU til reguleringsmyndigheter i De forente stater. Tilsvarende overføringer er tillatt til andre parter enn nevnte reguleringsmyndigheter, f.eks. foretak og andre forskere, i samsvar med prinsippene om opplysningsplikt og valgmulighet.

e. «Blindstudier»

i. For å gjøre kliniske utprøvinger så objektive som mulig får ikke deltakerne, og til tider heller ikke forskerne, innsyn i opplysninger om hvilken behandling hver av deltakerne får. Slikt innsyn kan sette forskningsstudiens og resultatenes gyldighet på spill. Det er ikke nødvendig å gi deltakere i slike kliniske utprøvinger (ofte kalt «blindstudier») innsyn i opplysninger om den behandlingen de får i løpet av utprøvingen, dersom denne begrensningen ble forklart da vedkommende samtykket i å delta i utprøvingen, og dersom innsyn i slike opplysninger vil være til skade for forskningsforsøkets integritet.

ii. Samtykke til å delta i utprøvingen på disse vilkårene anses som ensbetydende med at vedkommende frasier seg retten til innsyn. Når utprøvingen er avsluttet og resultatene analysert, skal deltakere gis innsyn i egne opplysninger dersom de ber om det. De bør først henvende seg til den legen eller behandleren som behandlet dem under den kliniske utprøvingen, og deretter eventuelt til organisasjonen som sponset utprøvingen.

f. Produktsikkerhet og overvåking av effekt

Et selskap som framstiller legemidler eller medisinsk utstyr, trenger ikke å anvende Privacy Shield-prinsippene om opplysningsplikt, valgmulighet, ansvar for videreoverføring og innsyn i sine aktiviteter knyttet til produktsikkerhet og overvåking av effekt, herunder rapportering av uønskede hendelser og sporing av pasienter/personer som bruker visse legemidler eller et visst medisinsk utstyr, når overholdelse av prinsippene kommer i konflikt med overholdelsen av

lovbestemte krav. Dette gjelder både for rapporter fra f.eks. helsetjenesteytere til selskaper som framstiller legemidler eller medisinsk utstyr, og for rapporter fra slike selskaper til offentlige organer, f.eks. De forente staters Food and Drug Administration.

g. Kodede opplysninger

Som regel koder den ansvarlige forskeren forskningsopplysningene ved kilden for ikke å avsløre den enkeltes identitet. Legemiddelforetak som sponser slik forskning, mottar ikke koden. Det er bare forskeren som har tilgang til den unike koden, slik at vedkommende under visse omstendigheter kan identifisere den enkelte deltaker (f.eks. ved behov for medisinsk oppfølging). En overføring fra EU til De forente stater av opplysninger som er kodet på denne måten, utgjør ikke en overføring av personopplysninger som er underlagt Privacy Shield-prinsippene.

15. **Offentlige registre og offentlig tilgjengelige opplysninger**

a. En organisasjon skal anvende Privacy Shield-prinsippene om sikkerhet, dataintegritet og formålsbegrensning samt klageadgang, håndheving og ansvar på offentlig tilgjengelige opplysninger. Disse prinsippene skal også anvendes på personopplysninger som samles inn fra offentlige registre, dvs. registre som forvaltes av offentlige organer eller enheter på ulike nivåer, og som er tilgjengelige for allmennheten.

b. Det er ikke nødvendig å anvende prinsippene om opplysningsplikt, valgmulighet eller ansvar for videreoverføring på opplysninger fra offentlige registre, så lenge de ikke kombineres med opplysninger fra registre som ikke er offentlige, og så lenge eventuelle vilkår for innsyn fastsatt av vedkommende myndighet oppfylles. Det er heller ikke nødvendig å anvende prinsippene om opplysningsplikt, valgmulighet eller ansvar for videreoverføring på offentlig tilgjengelige opplysninger, med mindre den europeiske avsenderen av opplysningene oppgir at de skal være underlagt begrensninger som krever at organisasjonen anvender disse prinsippene for de formålene opplysningene skal brukes til. Organisasjoner er ikke ansvarlige for hvordan slike opplysninger brukes av dem som innhenter slike opplysninger fra offentliggjort materiale.

c. Dersom det viser seg at en organisasjon med hensikt har offentliggjort personopplysninger i strid med prinsippene, slik at den eller andre kan dra nytte av disse unntakene, vil organisasjonen ikke lenger kunne dra nytte av fordelene ved Privacy Shield-ordningen.

d. Det er ikke nødvendig å anvende innsynsprinsippet på opplysninger fra offentlige registre, så lenge de ikke kombineres med andre personopplysninger (bortsett fra små mengder som brukes til indeksering eller organisering av opplysninger fra offentlige registre). Vilkår for innsyn fastsatt av vedkommende myndighet skal imidlertid overholdes. Når opplysninger fra offentlige registre kombineres med andre opplysninger som ikke er offentlig tilgjengelige (andre enn dem som er nevnt særskilt ovenfor), skal en organisasjon imidlertid gi innsyn i alle disse opplysningene såframt de ikke omfattes av andre unntak.

e. På samme måte som med opplysninger fra offentlige registre, er det ikke nødvendig å gi innsyn i opplysninger som allerede er offentlig tilgjengelige, så lenge de ikke kombineres med opplysninger som ikke er offentlig tilgjengelige. Organisasjoner som selger offentlig tilgjengelige opplysninger, kan kreve sitt ordinære gebyr ved anmodninger om innsyn. Privatpersoner kan også søke om innsyn i opplysninger om seg selv hos den organisasjonen som opprinnelig samlet inn opplysningene.

16. **Offentlige myndigheters anmodninger om tilgang**

a. For å sikre åpenhet i forbindelse med offentlige myndigheters lovlige anmodninger om tilgang til personopplysninger kan Privacy Shield-organisasjoner frivillig utarbeide regelmessige innsynsrapporter om antall anmodninger om personopplysninger som de mottar fra offentlige myndigheter med henblikk på rettshåndheving eller årsaker knyttet til nasjonal sikkerhet, i den grad utlevering av slike personopplysninger er tillatt i henhold til gjeldende rett.

b. Opplysningene som Privacy Shield-organisasjoner angir i slike rapporter sammen med opplysninger offentliggjort av etterretningssamfunnet og andre opplysninger, kan brukes i den årlige felles gjennomgåelsen av Privacy Shield-ordningens virkemåte i samsvar med prinsippene.

c. Manglende overholdelse av opplysningsplikten i samsvar med bokstav a) xii) i prinsippet om opplysningsplikt skal ikke hindre eller svekke en organisasjons evne til å svare på lovlige anmodninger.

———

Vedlegg I

Voldgiftsmodell

I dette vedlegg I angis vilkårene som Privacy Shield-organisasjoner plikter å rette seg etter for å avgjøre klager ved voldgift i henhold til prinsippet om klageadgang, håndheving og ansvar. Muligheten for tvungen voldgift beskrevet nedenfor får anvendelse på visse «resterende» krav vedrørende opplysninger som omfattes av Privacy Shield-avtalen mellom EU og De forente stater. Formålet med dette alternativet er å gi privatpersoner mulighet til å velge en rask, uavhengig og rettferdig mekanisme som kan behandle klager på påståtte overtredelser av prinsippene som ikke er blitt avgjort av eventuelle andre Privacy Shield-mekanismer.

A. **Virkeområde**

En privatperson har i forbindelse med resterende krav mulighet til å bringe saken inn for voldgift for å få fastslått om en Privacy Shield-organisasjon har misligholdt sine forpliktelser overfor vedkommende i henhold til prinsippene, og om det er truffet tiltak for helt eller delvis å korrigere dette. Dette alternativet er tilgjengelig bare for disse formålene. Dette alternativet er f.eks. ikke tilgjengelig i forbindelse med unntakene fra prinsippene([1]) eller når det gjelder påstander om hvorvidt det vernet som Privacy Shield-ordningen sikrer, er tilstrekkelig.

B. **Tilgjengelige rettsmidler**

Denne voldgiftsmuligheten gir Privacy Shield-panelet (som består av en eller tre voldgiftsmenn, avhengig av hva som er avtalt mellom partene) myndighet til å pålegge rimelige individuelle og ikke-økonomiske tiltak (f.eks. innsyn i, retting, sletting eller tilbakesending av vedkommendes opplysninger) som er nødvendige for å korrigere overtredelsen av prinsippene, utelukkende når det gjelder denne privatpersonen. Dette er voldgiftspanelets eneste myndighet når det gjelder rettsmidler. Voldgiftspanelet skal når det vurderer rettslige tiltak, ta høyde for andre rettslige tiltak som allerede er blitt pålagt gjennom andre mekanismer i Privacy Shield-ordningen. Ingen former for skadeserstatning, kostnader, gebyrer eller andre rettsmidler er tilgjengelige. Hver part skal betale sine egne advokatkostnader.

C. **Krav før voldgiftsbehandling**

En privatperson som beslutter å benytte denne voldgiftsmuligheten, skal gjøre følgende før krav framsettes: 1) Ta opp den påståtte overtredelsen direkte med organisasjonen og gi organisasjonen mulighet til å løse problemet innenfor tidsrammen fastsatt i avsnitt III nr. 11 bokstav d) i) i prinsippene, 2) benytte den uavhengige klagemekanismen i henhold til prinsippene, som skal være uten ekstra omkostninger for privatpersonen, og 3) via sin personvernmyndighet legge fram saken for det amerikanske handelsdepartementet og gi det mulighet til å gjøre sitt beste for å løse problemet innenfor tidsrammene fastsatt i brevet fra handelsdepartementets International Trade Administration uten ekstra omkostninger for vedkommende.

Det kan ikke framsettes krav om voldgift dersom den samme påståtte overtredelsen av prinsippene i henhold til prinsippene 1) tidligere har vært gjenstand for tvungen voldgift, 2) har vært gjenstand for en endelig dom avsagt i en rettssak som vedkommende var part i, eller 3) tidligere har vært gjenstand for forlik mellom partene. Denne muligheten kan heller ikke brukes dersom en personvernmyndighet i EU 1) har myndighet i henhold til avsnitt III nr. 5 eller III nr. 9 i prinsippene, eller 2) har myndighet til å avgjøre den påståtte overtredelsen direkte sammen med organisasjonen. En personvernmyndighets myndighet til å avgjøre den samme saken mot en behandlingsansvarlig i EU utelukker ikke alene muligheten til å framsette krav om voldgift overfor et annet rettssubjekt som ikke er bundet av personvernmyndighetens myndighet.

D. **Avgjørelsenes bindende karakter**

En person kan frivillig velge å anvende denne muligheten for tvungen voldgift. Voldgiftsavgjørelser er bindene for alle parter som deltar i voldgiftsprosessen. Når en privatperson har framsatt krav om voldgift, frasier vedkommende seg muligheten til å få samme påståtte overtredelse avgjort i et annet forum. Dersom rimelige ikke-økonomiske tiltak ikke avhjelper den påståtte overtredelsen fullt ut, utelukker det faktum at privatpersonen har framsatt krav om voldgift, imidlertid ikke muligheten til å kreve erstatning ved domstolene.

([1]) Avsnitt I nr. 5 i prinsippene.

E. **Kontroll og håndheving**

Privatpersoner og Privacy Shield-organisasjoner kan anmode om domstolskontroll og håndheving av voldgiftsavgjørelsene i henhold til amerikansk rett, nærmere bestemt Federal Arbitration Act([1]). Slike saker skal bringes inn for vedkommende føderale førsteinstansdomstol der hovedforretningsstedet til Privacy Shield-organisasjonen ligger.

Hensikten med voldgift er å løse individuelle tvister, det er ikke hensikten at voldgiftsavgjørelser skal fungere som overbevisende eller bindende presedens i saker der andre parter er involvert, herunder i framtidige voldgiftssaker for domstoler i EU eller De forente stater eller i FTC-saker.

F. **Voldgiftspanel**

Partene skal velge voldgiftsmenn på listen over voldgiftsmenn omhandlet nedenfor.

I samsvar med gjeldende rett skal det amerikanske handelsdepartementet og Europakommisjonen utarbeide en liste over minst 20 voldgiftsmenn valgt på grunnlag av uavhengighet, integritet og ekspertise. Det følgende får anvendelse i forbindelse med denne prosessen:

Voldgiftsmenn

1) oppføres på listen i en periode på tre år, bortsett fra ved ekstraordinære omstendigheter eller årsaker; denne treårsperioden kan fornyes én gang,

2) skal ikke motta instrukser fra eller være tilknyttet noen part eller noen Privacy Shield-organisasjon eller De forente stater, EU eller EU-medlemsstater eller andre offentlige myndigheter eller håndhevingsmyndigheter, og

3) skal ha rett til å arbeide som advokat i De forente stater og være ekspert på amerikansk personvernlovgivning, og ha ekspertkunnskap om EUs regelverk for vern av personopplysninger.

G. **Voldgiftsprosedyrer**

I henhold til gjeldende rett skal det amerikanske handelsdepartementet og Europakommisjonen innen seks måneder etter vedtakelse av beslutningen om tilstrekkelig beskyttelsesnivå komme til enighet om en rekke eksisterende og veletablerte amerikanske voldgiftsprosedyrer (f.eks. AAA eller JAMS) som skal få anvendelse på saker som bringes inn for Privacy Shield-panelet, idet det tas hensyn til følgende:

1. En privatperson kan innlede sak om tvungen voldgift, forutsatt at ovennevnte krav før voldgift er oppfylt, ved å sende en «melding» til organisasjonen. Meldingen skal inneholde et sammendrag av hva som er gjort i henhold til punkt C for å løse saken, en beskrivelse av den påståtte overtredelsen og – etter vedkommendes valg – eventuelle underlagsdokumenter og -materiale og/eller en analyse av den lovgivningen som får anvendelse på den påståtte overtredelsen.

([1]) I kapittel 2 i Federal Arbitration Act («FAA») fastslås det at «en voldgiftsavtale eller voldgiftskjennelse som følger av et juridisk forhold, avtalefestet eller ikke, som anses som kommersielt, herunder en transaksjon, kontrakt eller avtale beskrevet i [avsnitt 2 i FAA], faller inn under [Convention on the Recognition and Enforcement of Foreign Arbitral Awards av 10. juni 1958, 21 U.S.T. 2519, T.I.A.S. No 6997 («New York-konvensjonen»)].» 9 U.S.C. § 202. I FAA fastslås det videre «at en avtale eller kjennelse som følger av et slikt forhold, og som utelukkende eksisterer mellom amerikanske statsborgere, skal anses for ikke å falle inn under [New York]-konvensjonen, med mindre nevnte forhold omfatter eiendom i utlandet, skal gjennomføres eller håndheves i utlandet eller har en annen rimelig forbindelse til en eller flere fremmede stater.» Id. I henhold til kapittel 2 «kan enhver part i voldgiftssaken anmode enhver domstol med domsmyndighet i henhold til dette kapittel om en kjennelse som bekrefter voldgiftskjennelsen avsagt mot enhver annen part i voldgiftssaken. Domstolen skal bekrefte voldgiftskjennelsen, med mindre den konstaterer at en av grunnene til å nekte eller utsette anerkjennelsen eller fullbyrdelsen av voldgiftskjennelsen angitt i nevnte [New York]-konvensjon foreligger.» Id. § 207. I kapittel 2 fastslås det videre at «distriktsdomstolene i De forente stater … skal ha opprinnelig domsmyndighet over … saker [omfattet av New York-konvensjonen], uansett størrelsen på tvistebeløpet.» Id. § 203.
I kapittel 2 fastslås det også at «kapittel 1 får anvendelse på saker anlagt i henhold til dette kapittel i den grad det aktuelle kapittel ikke er i strid med dette kapittel eller [New York]-konvensjonen som ratifisert av De forente stater.» Id. § 208. I kapittel 1 fastslås det derimot at «en skriftlig bestemmelse i […] en kontrakt om en forretningsmessig transaksjon der en tvist som senere oppstår som følge av denne kontrakten eller transaksjonen eller nektelsen av å oppfylle hele eller deler av denne, skal avgjøres ved voldgift, eller en skriftlig avtale om at en eksisterende tvist oppstått som følge av en slik kontrakt, transaksjon eller nektelse skal avgjøres ved voldgift, er ugyldig, ugjenkallelig og tvangskraftig, med mindre det er andre grunner i henhold til loven eller billighetsprinsippet til å oppheve kontrakter.» Id. § 2. I kapittel 1 fastslås det videre at «enhver part i voldgiftssaken kan anmode vedkommende domstol om en kjennelse som bekrefter voldgiftskjennelsen, og at domstolen deretter skal avsi en slik kjennelse, med mindre voldgiftskjennelsen omstøtes, endres eller rettes som fastsatt i avsnitt 10 og 11 i [FAA].» Id. § 9.

2. Det vil bli utarbeidet prosedyrer for å sikre at den samme påståtte overtredelsen ikke omfattes av flere rettslige tiltak eller prosedyrer.

3. FTC-saker kan anlegges parallelt med voldgiftsbehandlingen.

4. Representanter for De forente stater, EU, EU-medlemsstater eller andre statlige organer, offentlige myndigheter eller håndhevingsmyndigheter kan ikke delta i disse voldgiftsbehandlingene. På anmodning fra en privatperson i EU kan personvernmyndigheter i EU bare bistå med utarbeidingen av meldingen, men kan ikke få tilgang til dokumenter eller annet materiale som gjelder voldgiftsbehandlingen.

5. Voldgiftsbehandlingen vil finne sted i De forente stater, og privatpersonen kan velge å delta via video- eller telefonkonferanse som skal stilles gratis til rådighet for vedkommende. Det er ikke nødvendig å møte opp personlig.

6. Med mindre partene har avtalt noe annet, skal voldgiftsbehandlingen foregå på engelsk. På en begrunnet anmodning og idet det tas hensyn til om privatpersonen representeres av en advokat eller ikke, vil både tolking under voldgiftshøringen og oversettelse av materiale knyttet til voldgiftssaken bli stilt gratis til rådighet for privatpersonen, med mindre panelet vurderer at dette i den aktuelle voldgiftssaken vil føre til uberettigede eller uforholdsmessig høye kostnader.

7. Materiale som legges fram for voldgiftsmenn, vil bli behandlet fortrolig og vil bare bli brukt i forbindelse med voldgiftsbehandlingen.

8. Individuell framlegging av dokumenter kan være tillatt ved behov, og dette vil bli behandlet fortrolig av partene og vil bare bli brukt i forbindelse med voldgiftsbehandlingen.

9. Voldgiftsbehandlingen bør avsluttes senest 90 dager etter at melding er gitt til den berørte organisasjonen, med mindre partene er blitt enige om noe annet.

H. **Kostnader**

Voldgiftsmenn bør treffe rimelige tiltak for å minimere voldgiftskostnadene eller -gebyrene.

Med forbehold for gjeldende rett vil det amerikanske handelsdepartementet i samråd med Europakommisjonen legge til rette for opprettelse av et fond som Privacy Shield-organisasjoner skal betale et årlig bidrag til, som dels er basert på organisasjonens størrelse, og som vil dekke voldgiftskostnadene, herunder honorar til voldgiftsmennene, opp til et maksimumsbeløp («tak»). Fondet vil bli forvaltet av en tredjepart som regelmessig skal rapportere om driften av fondet. Ved den årlige gjennomgåelsen vil det amerikanske handelsdepartementet og Europakommisjonen gjennomgå driften av fondet, herunder om det er behov for å justere bidragsbeløpene eller taket, samt blant annet vurdere antall voldgiftsbehandlinger og kostnadene for og varigheten av disse ut fra en gjensidig forståelse av at Privacy Shield-organisasjoner ikke må pålegges en urimelig stor økonomisk byrde. Advokathonorarer omfattes ikke av denne bestemmelsen eller av eventuelle fond i henhold til denne bestemmelsen.

———

VEDLEGG III

Brev fra John Kerry, De forente staters utenriksminister

7. juli 2016

Kjære kommissær Jourová

Det gleder meg at vi har kommet til en forståelse når det gjelder Privacy Shield-avtalen mellom Den europeiske union og De forente stater, som vil omfatte en ombudsmekanisme som myndigheter i EU kan inngi anmodninger til på vegne av privatpersoner i EU med hensyn til amerikansk signaletterretningspraksis.

President Barack Obama kunngjorde 17. januar 2014 en rekke viktige etterretningsreformer beskrevet i Presidential Policy Directive 28 (PPD-28). I henhold til PPD-28 har jeg utnevnt Catherine A. Novelli, statssekretær og seniorkoordinator for International Information Technology Diplomacy, som vårt kontaktpunkt for utenlandske regjeringer som ønsker å ta opp spørsmål om De forente staters signaletterretningsaktiviteter. På bakgrunn av dette har jeg opprettet en Privacy Shield-ombudsmekanisme i samsvar med vilkårene fastsatt i vedlegg A som er blitt oppdatert siden mitt brev av 22. februar 2016. Jeg har anmodet Catherine A. Novelli om å påta seg denne oppgaven. Statssekretær Novelli er uavhengig av det amerikanske etterretningssamfunnet og rapporterer direkte til meg.

Jeg har anmodet mine medarbeidere om å sette av de ressursene som er nødvendige for å innføre denne nye ombudsmekanismen, og jeg er sikker på at den vil bli et effektivt verktøy for å behandle spørsmål fra privatpersoner i EU.

Vennlig hilsen

John F. Kerry

Vedlegg A

Ombudsmekanismen i Privacy Shield-avtalen mellom EU og De forente stater med hensyn til signaletterretning

Tatt i betraktning viktigheten av rammeverket for Privacy Shield-avtalen mellom EU og De forente stater redegjøres det i dette memorandum for prosessen for innføring av en ny mekanisme, som er i samsvar med Presidential Policy Directive 28 (PPD-28), med hensyn til signaletterretning([1]).

17. januar 2014 holdt president Obama en tale der han kunngjorde viktige etterretningsreformer. I talen understreket han at De forente staters innsats ikke bare bidrar til å beskytte De forente stater, men også venner og allierte, og at vår innsats bare vil være effektiv dersom vanlige borgere i andre land kan stole på at De forente stater også respekterer deres privatliv. President Obama kunngjorde utstedelsen av et nytt presidentdirektiv – PPD-28 – for tydelig å fastsette hva vi gjør, og ikke gjør, når det gjelder oversjøisk overvåking.

I henhold til avsnitt 4 (d) i PPD-28 skal den amerikanske utenriksministeren utpeke en seniorkoordinator for International Information Technology Diplomacy («seniorkoordinator») som skal fungere som kontaktpunkt for utenlandske regjeringer som ønsker å ta opp spørsmål om De forente staters signaletterretningsaktiviteter. Statssekretær C. Novelli har fungert som seniorkoordinator siden januar 2015.

Dette memorandum inneholder en beskrivelse av en ny mekanisme som seniorkoordinatoren skal anvende for å lette behandlingen av anmodninger om tilgang til opplysninger overført fra EU til De forente stater innenfor rammen av Privacy Shield-ordningen for formål knyttet til nasjonal sikkerhet, standardavtalevilkår, bindende virksomhetsregler, «unntak»([2]) eller «mulige framtidige unntak»([3]), gjennom kanaler etablert i samsvar med gjeldende lover og politikk i De forente stater, samt hvordan slike anmodninger skal besvares.

1. **Privacy Shield-ombudet.** Seniorkoordinatoren vil fungere som Privacy Shield-ombud og, dersom det er relevant, utpeke ytterligere tjenestemenn i det amerikanske utenriksdepartementet som skal bistå henne med å utføre oppgavene som det redegjøres nærmere for i dette memorandum. (Koordinatoren og tjenestemenn som utfører slike oppgaver, vil heretter bli kalt «Privacy Shield-ombud».) Privacy Shield-ombudet vil samarbeide tett med relevante tjenestemenn fra andre departementer og byråer med ansvar for å behandle anmodninger i samsvar med gjeldende rett og politikk i De forente stater. Ombudet er uavhengig av etterretningssamfunnet. Ombudet rapporterer direkte til den amerikanske utenriksministeren som skal sikre at ombudet utfører sine oppgaver på en objektiv måte og uten utilbørlig påvirkning som kan ha innflytelse på svaret som skal gis.

2. **Effektiv samordning.** Privacy Shield-ombudet kan bruke tilsynsorganene beskrevet nedenfor og samordne dem på en effektiv måte for å sikre at ombudets svar på anmodninger som inngis av EU-klagebehandlingsorganet, er basert på

([1]) Forutsatt at kommisjonsbeslutningen om tilstrekkelig beskyttelsesnivå som sikres ved Privacy Shield-avtalen mellom EU og De forente stater, får anvendelse på Island, Liechtenstein og Norge, vil Privacy Shield-pakken omfatte både Den europeiske union og disse tre statene. Når det vises til EU og EUs medlemsstater, omfatter dette derfor også Island, Liechtenstein og Norge.

([2]) Med «unntak» i denne sammenhengen menes en eller flere kommersielle overføringer som finner sted forutsatt at a) den registrerte har gitt sitt uttrykkelige samtykke til den foreslåtte overføringen, eller b) overføringen er nødvendig for å oppfylle en avtale mellom den registrerte og den behandlingsansvarlige eller for å gjennomføre tiltak før avtaleinngåelse som treffes på den registrertes anmodning, eller c) overføringen er nødvendig for å inngå eller oppfylle en avtale inngått i den registrertes interesse mellom den behandlingsansvarlige og en tredjepart, eller d) overføringen er nødvendig eller lovpålagt for å verne en viktig samfunnsinteresse eller for å fastsette, gjøre gjeldende eller forsvare rettslige krav, eller e) overføringen er nødvendig for å verne den registrertes vitale interesser, eller f) overføringen gjøres fra et register som i henhold til lover eller forskrifter er ment å gi informasjon til allmennheten, og som er tilgjengelig enten for allmennheten eller for enhver person som kan vise en berettiget interesse, i den grad de lovfestede vilkårene for innsyn er oppfylt i det bestemte tilfellet.

([3]) Med «mulige framtidige unntak» menes i denne sammenheng en eller flere kommersielle overføringer som finner sted på et av følgende vilkår, i den grad vilkåret utgjør en lovlig grunn for overføring av personopplysninger fra EU til De forente stater: a) Den registrerte har gitt sitt uttrykkelige samtykke til den foreslåtte overføringen etter å ha blitt informert om de mulige risikoene som slike overføringer kan medføre for den registrerte på grunn av en manglende beslutning om tilstrekkelig beskyttelsesnivå og egnede garantier, eller b) overføringen er nødvendig for å verne den registrertes eller andre personers vitale interesser, dersom den registrerte ikke fysisk eller juridisk er i stand til å gi samtykke, eller c) ved en overføring til en tredjestat eller en internasjonal organisasjon og ingen av de andre unntakene eller mulige framtidige unntakene får anvendelse, bare dersom overføringen ikke er gjentakende, bare gjelder et begrenset antall registrerte, er nødvendig for å oppfylle den behandlingsansvarliges tvingende berettigede interesser, og den registrertes interesser eller rettigheter og friheter ikke veier tyngre, og den behandlingsansvarlige har vurdert alle forhold rundt dataoverføringen og på grunnlag av denne vurderingen har gitt egnede garantier med hensyn til vern av personopplysninger.

nødvendig informasjon. Dersom anmodningen gjelder hvorvidt overvåkingen er forenlig med amerikansk rett, vil Privacy Shield-ombudet kunne samarbeide med et av de uavhengige tilsynsorganene med undersøkelsesmyndighet.

a. Privacy Shield-ombudet vil samarbeide tett med andre representanter for den amerikanske regjering, herunder relevante uavhengige tilsynsorganer, for å sikre at utfylte anmodninger behandles og besvares i samsvar med gjeldende lover og politikk. Privacy Shield-ombudet vil ha mulighet til å sikre tett samordning med Office of the Director of National Intelligence, det amerikanske justisdepartementet og, når det er relevant, andre departementer og byråer som er involvert i De forente staters nasjonale sikkerhet, og generalinspektører, tjenestemenn med ansvar for gjennomføring av Freedom of Information Act og ansvarlige for borgerlige frihetsrettigheter og personvern («civil liberties and privacy officers»).

b. Den amerikanske regjering vil anvende mekanismer for samordning av og tilsyn med nasjonale sikkerhetsanliggender på tvers av departementer og byråer for å bidra til å sikre at Privacy Shield-ombudet i henhold til avsnitt 4 bokstav e) kan besvare utfylte anmodninger i henhold til avsnitt 3 bokstav b).

c. Privacy Shield-ombudet kan bringe spørsmål knyttet til anmodninger inn for Privacy and Civil Liberties Oversight Board.

3. **Inngivelse av anmodninger**

a. Enhver anmodning skal først inngis til tilsynsmyndighetene i medlemsstatene som fører tilsyn med nasjonale sikkerhetstjenester og/eller offentlige myndigheters behandling av personopplysninger. Anmodningen inngis til ombudet av et sentralisert EU-organ (heretter samlet kalt «EU-klagebehandlingsorganet»).

b. EU-klagebehandlingsorganet skal sikre at anmodningen er fullstendig på følgende måte:

i) Kontrollere personens identitet og at vedkommende opptrer på egne vegne og ikke som representant for en statlig eller mellomstatlig organisasjon.

ii) Sikre at anmodningen inngis skriftlig og at den inneholder følgende grunnleggende informasjon:

— All informasjon som danner grunnlaget for anmodningen.

— Informasjonens art eller ønsket løsning.

— Amerikanske statlige organer som antas å være involvert.

— Andre tiltak som er truffet for å oppnå den ønskede informasjonen eller løsningen, og utfallet av disse tiltakene.

iii) Kontrollere at anmodningen gjelder opplysninger som med rimelighet kan antas å være overført fra EU til De forente stater innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, standardavtalevilkår, bindende virksomhetsregler, unntak eller mulige framtidige unntak.

iv) Treffe en foreløpig beslutning om at anmodningen ikke er grunnløs, useriøs eller inngitt i ond tro.

c. For at en anmodning skal kunne behandles videre av Privacy Shield-ombudet i henhold til dette memorandum, er det ikke nødvendig å dokumentere i anmodningen at den amerikanske regjering rent faktisk har hatt tilgang til den anmodende partens opplysninger gjennom signaletterretningsaktiviteter.

4. **Forpliktelser med hensyn til kommunikasjon med EU-klagebehandlingsorganet som inngir en anmodning**

a. Privacy Shield-ombudet skal bekrefte mottak av anmodningen til EU-klagebehandlingsorganet som inngir en anmodning.

b. Privacy Shield-ombudet skal foreta en første gjennomgåelse for å sikre at anmodningen er utfylt i samsvar med avsnitt 3 bokstav b). Dersom Privacy Shield-ombudet oppdager mangler i eller har spørsmål om anmodningen, skal ombudet forsøke å løse disse problemene i samarbeid med EU-klagebehandlingsorganet som inngir anmodningen.

c. Dersom Privacy Shield-ombudet for å fremme behandlingen av anmodningen har behov for mer informasjon om anmodningen, eller dersom privatpersonen som opprinnelig innga anmodningen, må treffe særlige tiltak, skal Privacy Shield-ombudet underrette EU-klagebehandlingsorganet som har inngitt anmodningen.

d. Privacy Shield-ombudet vil spore status for anmodningene og ved behov legge fram oppdateringer for EU-klagebehandlingsorganet som har inngitt anmodningen.

e. Når en anmodning er utfylt som beskrevet i avsnitt 3 i dette memorandum, vil Privacy Shield-ombudet gi et rettidig og egnet svar til EU-klagebehandlingsorganet som har inngitt anmodningen, idet det tas hensyn til den løpende forpliktelsen om å verne opplysninger i henhold til gjeldende lover og politikk. Privacy Shield-ombudet vil svare EU-klagebehandlingsorganet som har inngitt anmodningen, med en bekreftelse på at i) klagen er blitt behørig undersøkt, og ii) at amerikansk rett, lover, presidentordrer, presidentdirektiver og byråretningslinjer, idet det tas hensyn til begrensningene og garantiene beskrevet i brevet fra ODNI, er overholdt, eller at en eventuell manglende overholdelse er blitt korrigert. Privacy Shield-ombudet vil verken bekrefte eller avkrefte at personen har vært et mål for overvåking, eller bekrefte hvilket spesifikt rettsmiddel som er blitt anvendt. Som forklart nærmere i avsnitt 5 vil FOIA-anmodninger bli behandlet som fastsatt i denne loven og gjeldende bestemmelser.

f. Privacy Shield-ombudet vil kommunisere direkte med EU-klagebehandlingsorganet, som igjen vil ha ansvar for å kommunisere med privatpersonen som inngir anmodningen. Dersom direkte kommunikasjon er en del av de underliggende prosessene beskrevet nedenfor, vil slik kommunikasjon finne sted i samsvar med eksisterende framgangsmåter.

g. De forpliktende tilsagnene i dette memorandum får ikke anvendelse på generelle påstander om at Privacy Shield-avtalen mellom EU og De forente stater er i strid med Den europeiske unions krav til vern av personopplysninger. De forpliktende tilsagnene i dette memorandum er avgitt på grunnlag av Europakommisjonens og den amerikanske regjerings felles forståelse av at det som følge av nevnte tilsagns omfang i henhold til denne mekanismen, kan oppstå ressursbegrensninger, herunder med hensyn til anmodninger i henhold til Freedom of Information Act (FOIA). Dersom utøvelsen av Privacy Shield-ombudets funksjoner i betydelig grad overskrider rimelige ressursbegrensninger og gjør det umulig å oppfylle disse forpliktelsene, vil den amerikanske regjering drøfte relevante justeringer for å rette opp situasjonen med Europakommisjonen.

5. **Anmodninger om informasjon.** Anmodninger om innsyn i den amerikanske regjerings registre kan inngis og behandles i henhold til Freedom of Information Act (FOIA).

a. FOIA gjør det mulig for enhver person, uavhengig av vedkommendes statsborgerskap, å søke om innsyn i føderale byråers eksisterende registre. Denne loven er kodifisert i United States Code (5 U.S.C. § 552). Loven og ytterligere informasjon om FOIA er tilgjengelig på www.FOIA.gov og http://www.justice.gov/oip/foia-resources. Hvert byrå har en Chief FOIA Officer og har på sitt offentlige nettsted lagt ut informasjon om hvordan FOIA-anmodninger inngis til byrået. Byråene har innført prosesser for å rådføre seg med hverandre om FOIA-anmodninger som omfatter registre i andre byråer.

b. Eksempler:

i) Office of the Director of National Intelligence (ODNI) har opprettet «ODNI FOIA-portalen» for ODNI: http://www.dni.gov/index.php/about-this-site/foia. Denne portalen inneholder informasjon om hvordan man inngir en anmodning, kontrollerer status for en eksisterende anmodning og får tilgang til informasjon som er utgitt og publisert av ODNI i henhold til FOIA. ODNI FOIA-portalen har lenker til andre FOIA-nettsteder for enheter innen etterretningssamfunnet: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Justisdepartementets Office of Information Policy stiller til rådighet omfattende informasjon om FOIA: http://www.justice.gov/oip. Dette omfatter ikke bare informasjon om hvordan en FOIA-anmodning inngis til justisdepartementet, men også veiledning til den amerikanske regjering om fortolkning og anvendelse av FOIA-krav.

c. I henhold til FOIA er innsyn i offentlige myndigheters registre omfattet av visse angitte unntak. Disse omfatter begrensninger når det gjelder innsyn i gradert informasjon knyttet til nasjonal sikkerhet, tredjeparters personopplysninger og informasjon som gjelder etterforskning i forbindelse med rettshåndheving, og kan sammenlignes med de begrensningene som de enkelte EU-medlemsstatene pålegger i sine egne lover om innsyn. Disse begrensningene gjelder både for amerikanske og ikke-amerikanske personer.

d. Tvister om utlevering av registre som det anmodes om i henhold til FOIA, kan påklages administrativt og deretter ved føderale domstoler. Domstolen skal treffe en **de novo**-avgjørelse om hvorvidt registrene holdes tilbake på lovlig vis (5 U.S.C. § 552 (a) (4) (B)), og kan tvinge offentlige myndigheter til å gi innsyn i registre. I noen tilfeller har domstoler omstøtt myndighetenes avgjørelser om at informasjon ikke skal utleveres fordi den er gradert. Selv om det ikke gis skadeserstatning, kan domstolene tilkjenne et beløp til dekning av advokathonorarer.

6. **Anmodninger om ytterligere tiltak.** En anmodning med påstand om lovovertredelse eller annen tjenesteforsømmelse vil bli henvist til vedkommende amerikanske offentlige organ, herunder uavhengige tilsynsorganer, med myndighet til å undersøke den aktuelle anmodningen og gripe inn ved manglende overholdelse som beskrevet nedenfor.

a. Generalinspektører («Inspectors Generals») har lovfestet uavhengighet og omfattende myndighet til å foreta undersøkelser, revisjoner og gjennomgåelser av programmer, herunder om bedrageri og misbruk eller overtredelse av loven, og kan anbefale korrigerende tiltak.

i) Ved Inspector General Act fra 1978 med etterfølgende endringer ble det opprettet uavhengige og objektive enheter, føderale generalinspektører, i de fleste byråer. Deres oppgave er å bekjempe sløsing, bedrageri og misbruk i de respektive byråenes programmer og virksomhet. Generalinspektørene har i denne forbindelse ansvar for å gjennomføre revisjoner og undersøkelser knyttet til eget byrås programmer og virksomhet. Generalinspektørene sørger også for ledelse og samordning og anbefaler retningslinjer for aktiviteter med henblikk på å fremme sparsomhet, produktivitet og effektivitet samt forebygging og avsløring av bedrageri og misligheter i byråets programmer og virksomhet.

ii) Hver enhet innen etterretningssamfunnet har sitt eget generalinspektørkontor (Office of the Inspector General) med ansvar for å føre tilsyn med blant annet utenlandsetterretningsaktiviteter. En rekke rapporter fra generalinspektørene om etterretningsprogrammer er offentliggjort.

iii) Eksempler:

— Office of the Inspector General of the Intelligence Community (IC IG) ble opprettet i henhold til avsnitt 405 i Intelligence Authorization Act of Fiscal Year 2010 (http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf). IC IG har ansvar for å utføre revisjoner, undersøkelser, inspeksjoner og gjennomgåelser av det amerikanske etterretningssamfunnet med henblikk på å identifisere og håndtere systemrelaterte risikoer, sårbare områder og svakheter som er knyttet til etterretningsbyråenes oppdrag, med det som mål å bedre etterretningssamfunnets økonomi og effektivitet. IC IG har myndighet til å undersøke klager eller informasjon om påståtte overtredelser av lover, regler og forskrifter samt påstander om sløsing, bedrageri, maktmisbruk eller en alvorlig eller spesifikk fare for folkehelsen og den offentlig sikkerhet i forbindelse med ODNIs og/eller etterretningssamfunnets etterretningsprogrammer og -aktiviteter. Informasjon om hvordan IC IG kan kontaktes direkte for å inngi en rapport finnes på nettstedet til IC IG: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Office of the Inspector General (OIG) i det amerikanske justisdepartementet (https://www.justice.gov) er en uavhengig enhet opprettet ved lov som har som oppgave å avsløre og forebygge sløseri, bedrageri, misbruk og feil i justisdepartementets programmer og blant departementets personell, og å fremme økonomi og effektivitet i disse programmene. OIG undersøker påståtte straffe- og sivilrettslige overtredelser begått av justisdepartementets ansatte og reviderer og inspiserer også departementets programmer. OIG har myndighet til å behandle alle klager på tjenesteforsømmelse begått av justisdepartementets 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 som arbeider i andre avdelinger eller på kontorer i justisdepartementet. (Det eneste unntaket er at påstander om tjenesteforsømmelse begått av en av departementets jurister eller rettshåndhevingstjenestemenn og som er knyttet til utøvelsen av juristens myndighet til å undersøke, gå til sak eller yte juridisk bistand, hører inn under

departementets Office of Professional Responsibility.) I henhold til avsnitt 1001 i USA Patriot Act, som ble undertegnet 26. oktober 2001, skal generalinspektøren gjennomgå informasjon og motta klager med påstand om krenkelser av borgerrettigheter og borgerlige frihetsrettigheter begått av justisdepartementets ansatte. OIG har et offentlig nettsted (https://www.oig.justice.gov) med en «direktelinje» for inngivelse av klager (https://www.oig.justice.gov/hotline/index.htm).

b. Den amerikanske regjerings kontorer og enheter med ansvar for personvern og borgerlige frihetsrettigheter har også relevante ansvarsområder. Eksempler:

i) Ved avsnitt 803 i Implementing Recommendations of the 9/11 Commission Act fra 2007, kodifisert i United States Code i 42 U.S.C. § 2000-ee1, utnevnes det ansvarlige for personvern og borgerlige frihetsrettigheter («privacy and civil liberties officers») i visse departementer og byråer (herunder utenriksdepartementet, justisdepartementet og ODNI). I avsnitt 803 presiseres det at disse ansvarlige for personvern og borgerlige frihetsrettigheter skal være hovedrådgivere for bl.a. å sikre at disse departementene, byråene eller enhetene har innført egnede framgangsmåter for å håndtere klager fra privatpersoner som påstår at et departement, et byrå eller en enhet har krenket deres personvern eller borgerlige frihetsrettigheter.

ii) ODNIs Civil Liberties and Privacy Office (ODNI CLPO) ledes av ODNI Civil Liberties Protection Officer, en stilling som ble opprettet ved National Security Act fra 1948 med etterfølgende endringer. ODNI CLPO har blant annet som oppgave å sikre at retningslinjene og prosedyrene til enhetene i etterretningssamfunnet i tilstrekkelig grad ivaretar personvernet og de borgerlige frihetsrettighetene, og å gjennomgå og undersøke klager med påstand om misbruk eller krenkelse av borgerlige frihetsrettigheter og personvern i ODNIs programmer og aktiviteter. ODNI CLPO stiller informasjon til rådighet for allmennheten på sitt nettsted, herunder om inngivelse av klager: www.dni.gov/clpo. Dersom ODNI CLPO mottar en klage på krenkelse av personvernet eller de borgerlige frihetsrettighetene som omfatter etterretningssamfunnets programmer og aktiviteter, skal ODNI CLPO sammen med andre enheter i etterretningssamfunnet samordne hvordan klagen skal behandles videre i etterretnings-samfunnet. National Security Agency (NSA) har også et Civil Liberties and Privacy Office som har et nettsted med informasjon om sine ansvarsområder (https://www.nsa.gov/civil_liberties/). Dersom informasjonen angir at et byrå ikke oppfyller kravene med hensyn til personvern (f.eks. et krav i henhold til avsnitt 4 i PPD-28), har byråene mekanismer som skal sikre at prinsippene overholdes, og at hendelsen gjennomgås og korrigeres. Byråene skal rapportere om tilfeller av manglende overholdelse i henhold til PPD-28 til ODNI.

iii) Office of Privacy and Civil Liberties (OPCL) i justisdepartementet bistår departementets Chief Privacy and Civil Liberties Officer (CPCLO) i dennes oppgaver og ansvarsområder. OPCLs hovedoppgave er å verne den amerikanske befolkningens personvern og borgerlige frihetsrettigheter ved å gjennomgå, føre tilsyn med og samordne departementets personvernaktiviteter. OPCL yter juridisk bistand og veiledning til departementets enheter, sikrer at departementet oppfyller bestemmelsene om personvern, herunder i Privacy Act fra 1974, personvernbestemmelsene i både E-Government Act fra 2002 og Federal Information Security Management Act, samt forvaltningspolitiske direktiver utstedt i henhold til disse lovene, utvikler og gir opplæring om personvern til departementets ansatte, bistår CPCLO med å utarbeide departementets personvernprogram, utarbeider personvernrelaterte rapporter til presidenten og Kongressen og gjennomgår departementets informasjons-håndteringspraksis for å sikre at den ikke er i strid med de borgerlige frihetsrettighetene og personvernet. OPCL informerer allmennheten om sine ansvarsområder på nettstedet http://www.justice.gov/opcl.

iv) I henhold til 42 U.S.C. § 2000ee *et seq.* skal Privacy and Civil Liberties Oversight Board løpende gjennomgå i) retningslinjene og prosedyrene, samt gjennomføringen av disse, til departementene, byråene og enhetene innen den utøvende gren som gjelder tiltak for å beskytte nasjonen mot terrorisme med det formål å sikre at personvernet og de borgerlige frihetsrettigheter ikke krenkes, og ii) andre tiltak fra den utøvende makt med det formål å bestemme om slike tiltak i tilstrekkelig grad ivaretar personvernet og de borgerlige frihetsrettighetene og er i samsvar med gjeldende lover, regler og retningslinjer på området personvern og borgerlige frihetsrettigheter. Det skal motta og gjennomgå rapporter og annen informasjon fra ansvarlige for personvern og borgerlige frihetsrettigheter og, dersom det er relevant, utstede anbefalinger til dem om deres aktiviteter. I henhold til avsnitt 803 i Implementing Recommendations of the 9/11 Commission Act fra 2007, kodifisert i 42 U.S.C. § 2000ee-1, skal ansvarlige for personvern og borgerlige frihetsrettigheter i åtte føderale byråer (herunder forsvarsministeren (Secretary of Defense), ministeren for nasjonal sikkerhet (Secretary of Homeland Security), direktøren for National Intelligence og direktøren for Central Intelligence Agency) og eventuelle andre byråer som er utpekt av PCLOB, inngi

periodiske rapporter til PCLOB, herunder om antall og arten av samt innholdet i klagene på påståtte overtredelser som det enkelte byrå har mottatt. I henhold til fullmaktsloven for PCLOB skal PCLOB motta disse rapportene og, dersom det er relevant, utstede anbefalinger til ansvarlige for personvern og borgerlige frihetsrettigheter med hensyn til deres aktiviteter.

———

VEDLEGG IV

Brev fra Edith Ramirez, leder for Federal Trade Commission

7. juli 2016

VIA E-POST

Věra Jourová
Kommissær for justis, forbrukersaker og likestilling
Europakommisjonen
Rue de la Loi / Wetstraat 200
1049 Brussel
Belgia

Kjære kommissær Jourová

De forente staters Federal Trade Commission («FTC») er glad for muligheten til å redegjøre for sin håndheving av det nye rammeverket for Privacy Shield-avtalen mellom EU og De forente stater («Privacy Shield-rammeverket» eller «rammeverket»). Vi mener at rammeverket vil komme til å spille en avgjørende rolle når det gjelder å fremme vern av personopplysninger som overføres i forbindelse med kommersielle transaksjoner i en stadig mer sammenkoplet verden. Det vil gi foretak mulighet til å gjennomføre viktige transaksjoner i den globale økonomien og samtidig sikre et fortsatt sterkt vern av personopplysningene til forbrukere i EU. FTC har lenge arbeidet for å sikre vern av personopplysninger på tvers av grensene og vil prioritere håndhevingen av det nye rammeverket høyt. Nedenfor redegjør vi for FTCs sterke håndheving av personvernet generelt, herunder vår håndheving av det opprinnelige «trygg havn»-programmet, og for FTCs strategi for å håndheve det nye rammeverket.

FTC forpliktet seg første gang offentlig til å håndheve «trygg havn»-programmet i år 2000. Tidligere leder for FTC, Robert Pitofsky, sendte på dette tidspunktet et brev til Europakommisjonen der han redegjorde for at FTC forpliktet seg til å håndheve «trygg havn»-prinsippene for personvern strengt. FTC har oppfylt denne forpliktelsen gjennom nesten 40 håndhevingstiltak, en rekke ytterligere undersøkelser og samarbeid med individuelle personvernmyndigheter i EU om spørsmål av gjensidig interesse.

Etter at Europakommisjonen i november 2013 uttrykte bekymring over forvaltningen og håndhevingen av «trygg havn»-programmet, innledet vi og det amerikanske handelsdepartementet drøftinger med representanter fra Europakommisjonen for å finne ut hvordan programmet kunne styrkes. Samtidig med disse drøftingene traff Den europeiske unions domstol 6. oktober 2015 en avgjørelse i *Schrems*-saken som bl.a. gjorde Europakommisjonens vedtak om tilstrekkeligheten av «trygg havn»-programmet ugyldig. Etter denne avgjørelsen fortsatte vi å samarbeide tett med handelsdepartementet og Europakommisjonen med henblikk på å styrke personvernet for privatpersoner i EU. Privacy Shield-rammeverket er et resultat av disse løpende drøftingene. På samme måte som med «trygg havn»-programmet forplikter FTC seg herved til å håndheve det nye rammeverket strengt. Dette brevet formaliserer denne forpliktelsen.

Vi bekrefter særlig våre forpliktende tilsagn på fire hovedområder: 1) Prioritering og undersøkelse av henviste saker, 2) håndtering av falske eller villedende påstander om deltakelse i Privacy Shield-ordningen, 3) løpende overvåking av pålegg og 4) økt engasjement og samarbeid med EUs personvernmyndigheter. Nedenfor redegjør vi nærmere for de enkelte forpliktelsene og relevant bakgrunn for FTCs rolle når det gjelder å sikre forbrukernes personvern samt håndheving av «trygg havn»-ordningen, og for det generelle «personvernlandskapet» i De forente stater([1]).

I. BAKGRUNN

A. **FTCs arbeid for å håndheve personvernet samt utarbeiding av strategi på dette området**

FTC har omfattende sivilrettslig håndhevingsmyndighet til å fremme forbrukervern og konkurranse på det kommersielle området. Som en del av sitt forbrukervernmandat håndhever FTC en lang rekke lover med henblikk på vern av

([1]) Ytterligere informasjon om De forente staters føderale og delstatlige personvernlover er angitt i tillegg A. FTCs nettsted inneholder i tillegg en oppsummering av våre nylige håndhevingstiltak på området personvern og sikkerhet: https://www.ftc.gov/reports/privacy-data-security-update-2015.

forbrukeropplysninger. Den viktigste loven som håndheves av FTC, FTC Act, forbyr «urimelig» og «villedende» atferd eller praksis i forbindelse med handel([1]). En erklæring, en utelatelse eller en praksis er villedende dersom den er konkret og kan antas å villede forbrukere som opptrer fornuftig ut fra omstendighetene([2]). En atferd eller praksis er urimelig dersom den forårsaker, eller kan antas å forårsake, vesentlig skade for forbrukerne som med rimelighet ikke kan unngås, og som ikke oppveies av andre fordeler for forbrukerne eller konkurransen([3]). FTC håndhever også målrettede lover om vern av opplysninger knyttet til helse, kreditt eller andre finansielle spørsmål, og om elektroniske opplysninger om barn, og har utstedt lovregler som gjennomfører hver av disse lovene.

FTCs myndighet i henhold til FTC Act omfatter saker «i forbindelse med handel». FTC har ingen myndighet på området strafferettslig håndheving eller nasjonale sikkerhetsanliggender. De fleste andre statlige tiltak faller heller ikke inn under FTCs myndighet. Det er i tillegg en rekke unntak når det gjelder FTCs myndighet på området forretningsvirksomhet, herunder med hensyn til banker, luftfartsselskaper, forsikringsvirksomhet og de vanlige aktivitetene til leverandører av telekommunikasjon. FTC har heller ingen myndighet over de fleste ideelle organisasjoner, men har derimot myndighet over falske veldedige organisasjoner eller andre ideelle organisasjoner som rent faktisk arbeider for å oppnå fortjeneste. FTC har også myndighet over ideelle organisasjoner som arbeider for å oppnå fortjeneste for sine fortjenestesøkende medlemmer, herunder ved å gi betydelige økonomiske fordeler til disse medlemmene([4]). I noen tilfeller faller FTCs myndighet sammen med andre rettshåndhevende organers myndighet.

Vi har utviklet et sterkt samarbeid med føderale myndigheter og delstatsmyndigheter og samarbeider tett med dem for å samordne undersøkelser eller henvise saker når det er relevant.

Håndheving er krumtappen i FTCs tilnærming til personvern. FTC har hittil anlagt over 500 saker knyttet til vern av forbrukeropplysninger. Disse sakene gjelder både elektroniske og ikke-elektroniske opplysninger og omfatter håndhevingstiltak overfor store og små selskaper med påstand om at de ikke har slettet sensitive forbrukeropplysninger på riktig måte, ikke har sikret forbrukeres personopplysninger, ulovlig har sporet forbrukere på nettet, har sendt søppelpost til forbrukere, installert spionprogramvare eller annen ondsinnet programvare på forbrukernes datamaskiner, brutt de amerikanske «Do Not Call»-reglene og andre regler for telefonmarkedsføring og urettmessig har samlet inn og utvekslet forbrukeropplysninger på mobile enheter. FTCs håndhevingstiltak – både i den fysiske og digitale verdenen – sender et viktig budskap til selskaper om behovet for å sikre forbrukernes personvern.

FTC har også gjennomført flere politiske initiativer med det formål å øke forbrukernes personvern, som er grunnlaget for FTCs håndhevingsarbeid. FTC har avholdt seminarer og utstedt rapporter med anbefalinger om beste praksis med det formål å bedre personvernet i det mobile økosystemet, øke åpenheten i datameglingsbransjen, maksimere fordelene ved stordata og samtidig begrense risikoene ved dette, særlig for forbrukere med lav inntekt og forbrukere som ikke har tilstrekkelig tilgang til tjenester, og understreke personvern- og sikkerhetsrelaterte konsekvenser av bl.a. ansiktsgjenkjenning og «tingenes internett».

FTC driver også opplysningsvirksomhet rettet mot forbrukere og virksomheter for å øke virkningene av sitt håndhevingsarbeid og utarbeiding av politiske initiativer. FTC har benyttet en rekke forskjellige verktøyer – publikasjoner, nettbaserte ressurser, seminarer og sosiale medier – for å gjøre tilgjengelig opplæringsmateriale om en rekke emner, herunder mobilapper, barns personvern og datasikkerhet. Nylig lanserte FTC «Start With Security»-initiativet med ny rettledning for virksomheter som bygger på tidligere erfaringer fra byråets saker om datasikkerhet samt en rekke seminarer rundt om i landet. FTC har dessuten lenge vært ledende innen opplæring av forbrukere om grunnleggende datasikkerhet. I fjor hadde vårt nettsted OnGuard Online og det spanskspråklige motstykket Alerta en Línea over 5 millioner sidevisninger.

B. **Rettslig vern i De forente stater som forbrukere i EU drar nytte av**

Ordningen vil fungere innenfor rammen av de generelle personvernreglene som gjelder i De forente stater, og som beskytter forbrukere i EU på en rekke måter.

([1]) 15 U.S.C. § 45 (a).

([2]) Se FTC Policy Statement on Deception, vedlagt Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), tilgjengelig på 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, vedlagt Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), tilgjengelig på 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).

Forbudet i FTC Act mot urimelig eller villedende atferd eller praksis beskytter ikke bare amerikanske forbrukere mot amerikanske selskaper, ettersom loven også omfatter praksis som 1) forårsaker eller vil kunne forårsake skade i De forente stater som med rimelighet kan forutses, eller 2) omfatter en konkret atferd i De forente stater. For å beskytte utenlandske forbrukere kan FTC dessuten bruke alle rettsmidler, herunder restitusjon, som er tilgjengelige for å beskytte amerikanske forbrukere.

FTCs håndhevingsarbeid gagner både amerikanske og utenlandske forbrukere. Våre saker om håndheving av avsnitt 5 i FTC Act har f.eks. sørget for at både amerikanske og utenlandske forbrukeres personvern er blitt ivaretatt. I en sak mot en informasjonsmegler, Accusearch, hevdet FTC at selskapets salg av fortrolige telefonregistre til tredjeparter uten forbrukernes viten eller samtykke var en urimelig praksis i strid med avsnitt 5 i FTC Act. Accusearch solgte opplysninger om både amerikanske og utenlandske forbrukere([1]). Domstolen utstedte et rettslig pålegg mot Accusearch med bl.a. forbud mot markedsføring eller salg av forbrukeres personopplysninger uten skriftlig samtykke, med mindre opplysningene var lovlig innsamlede offentlig tilgjengelige opplysninger, og påla selskapet å betale en bot på nærmere 200 000 USD([2]).

FTCs forlik med TRUSTe er et annet eksempel. Det sikrer at forbrukere, herunder forbrukere i Den europeiske union, kan ha tillit til globale selvreguleringsorganisasjoners erklæringer om kontroll og sertifisering av nasjonale og utenlandske nettjenester([3]). Vår sak mot TRUSTe styrker dessuten selvreguleringssystemet for personvern mer generelt ved å sikre at enheter som spiller en viktig rolle i selvreguleringsordninger, herunder grensekryssende ordninger for personvern, stilles til ansvar.

FTC håndhever dessuten andre målrettede lover hvis bestemmelser om vern også får anvendelse på ikke-amerikanske forbrukere, f.eks. Children's Online Privacy Protection Act («COPPA»). I henhold til COPPA skal operatører av nettsteder og nettjenester rettet mot barn eller nettsteder rettet mot allmennheten som bevisst samler inn personopplysninger fra barn under 13 år, blant annet informere foreldrene og innhente et kontrollerbart samtykke fra foreldrene. USA-baserte nettsteder og -tjenester som omfattes av COPPA, og som samler inn personopplysninger fra utenlandske barn, skal overholde COPPA. Utenlandske nettsteder og nettjenester må også overholde COPPA dersom de er rettet mot barn i De forente stater, eller dersom de bevisst samler inn personopplysninger fra barn i De forente stater. I tillegg til amerikansk føderal rett som håndheves av FTC, kan det finnes visse andre lover på området forbrukervern og personvern på føderalt plan og delstatsplan som sikrer forbrukere i EU ytterligere fordeler.

C. **Håndheving av «trygg havn»-ordningen**

Som en del av sitt program for håndheving av reglene på området personvern og sikkerhet, har FTC også forsøkt å verne forbrukere i EU ved å anlegge saker om overtredelser av «trygg havn»-ordningen. FTC har anlagt 39 saker knyttet til «trygg havn»-ordningen: 36 saker om falske påstander om sertifisering og tre saker (mot Google, Facebook og Myspace) om påståtte overtredelser av «trygg havn»-prinsippene for personvern([4]). Disse sakene viser at sertifiseringer kan håndheves, og at manglende overholdelse får konsekvenser. Forliksavgjørelser («consent orders») med en varighet på 20 år krever at Google, Facebook og Myspace gjennomfører omfattende personvernprogrammer som må være utformet på en rimelig måte med henblikk på å håndtere personvernrisikoer knyttet til utvikling og forvaltning av nye og eksisterende produkter og tjenester, og for å sikre vern av personopplysninger og opplysningssikkerheten. De omfattende personvernprogrammene som skal gjennomføres i henhold til disse avgjørelsene, skal identifisere forutsigbare vesentlige risikoer og omfatte kontrolltiltak for å håndtere disse risikoene. Selskapene skal også oversende løpende og uavhengige vurderinger av sine personvernprogrammer til FTC. Avgjørelsene forbyr også disse selskapene å avgi uriktige opplysninger om egen personvernpraksis og deltakelse i personvern- eller sikkerhetsprogrammer. Dette forbudet får også anvendelse på selskapers atferd og praksis i henhold til det nye

([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 innga en amicus curiae-rapport i forbindelse med anken av FTC-saken og foretok sin egen undersøkelse og konkluderte med at Accusearchs praksis også var i strid med kanadisk rett.

([2]) Se FTC v. Accusearch, Inc., No 06CV015D (D. Wyo. 20. des. 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. 12. mars 2015) (avgjørelse og kjennelse), tilgjengelig på 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. 13. okt. 2011) (avgjørelse og kjennelse), tilgjengelig på 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. 27. juli 2012) (avgjørelse og kjennelse), tilgjengelig på 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. 30. aug. 2012) (avgjørelse og kjennelse), tilgjengelig på https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

Privacy Shield-rammeverket. FTC kan håndheve disse avgjørelsene ved å ilegge sivilrettslige sanksjoner. Google ble faktisk idømt en rekordstor bot på 22,5 millioner USD i 2012 etter påstander om at selskapet ikke hadde rettet seg etter avgjørelsen. Disse FTC-avgjørelsene bidrar til å beskytte over en milliard forbrukere over hele verden, hvorav flere hundre millioner er bosatt i Europa.

I FTCs saker har det også vært fokus på falske, bedragerske eller villedende påstander om deltakelse i «trygg havn»-ordningen. FTC tar disse påstandene alvorlig. I saken *FTC v. Karnani* anla FTC i 2011 f.eks. sak mot en internettmarkedsfører i De forente stater med påstand om at vedkommende og vedkommendes selskap villedet britiske forbrukere til å tro at selskapet var basert i Det forente kongerike, herunder ved å bruke domenenavnet .uk og ved å oppgi priser i britisk valuta og henvise til det britiske postsystemet([1]). Da forbrukerne mottok produktene, oppdaget de imidlertid uventede importavgifter, garantier som ikke var gyldige i Det forente kongerike, og omkostninger forbundet med å få pengene tilbake. FTC hevdet også at de saksøkte villedet forbrukerne med hensyn til deres deltakelse i «trygg havn»-ordningen. Alle de berørte forbrukerne befant seg i Det forente kongerike.

Mange av våre andre saker om håndheving av «trygg havn»-ordningen har omfattet organisasjoner som hadde sluttet seg til «trygg havn»-ordningen, men som ikke fornyet sin årlige sertifisering, men fortsatte å framstille seg selv som deltakere. Som beskrevet nærmere nedenfor arbeider FTC også for å bekjempe falske påstander om deltakelse i Privacy Shield-ordningen. Denne strategiske håndhevingsaktiviteten utfyller handelsdepartementets økte innsats for å kontrollere at programkravene for sertifisering og ny sertifisering overholdes, departementets overvåking av at kravene faktisk overholdes, herunder ved bruk av spørreskjemaer rettet til deltakere som deltar i ordningen, og dets økte innsats for å identifisere falske påstander om deltakelse i ordningen og misbruk av ordningens sertifiseringsmerke([2]).

II. PRIORITERING AV HENVISTE SAKER OG UNDERSØKELSER

På samme måte som under «trygg havn»-ordningen vil FTC prioritere saker som henvises fra EU-medlemsstatene innenfor rammen av Privacy Shield-ordningen. Vi vil også prioritere saker om manglende overholdelse av retningslinjene for selvregulering knyttet til Privacy Shield-rammeverket som henvises fra selvreguleringsorganisasjoner og andre uavhengige tvisteløsningsorganer på personvernområdet.

For å lette henvisningen av saker fra EU-medlemsstatene i henhold til rammeverket er FTC i ferd med å utarbeide en standardisert henvisningsprosess samt veiledning til EU-medlemsstater om hvilken type informasjon som gir FTC det beste grunnlaget for å undersøke en henvist sak. I forbindelse med dette vil FTC utpeke et internt kontaktpunkt for henvisninger fra EU-medlemsstatene. Det vil være til stor hjelp dersom henvisende myndighet foretar en forundersøkelse av den påståtte overtredelsen og kan samarbeide med FTC i en eventuell undersøkelse.

Etter mottak av en sak henvist fra en EU-medlemsstat eller en selvreguleringsorganisasjon kan FTC treffe en rekke tiltak med hensyn til de henviste sakene. Vi kan f.eks. gjennomgå selskapets personvernprogrammer, innhente mer informasjon direkte fra selskapet eller fra tredjeparter, følge opp saken med henvisende instans, vurdere om overtredelsene inngår i et mønster eller omfatter et betydelig antall berørte forbrukere, vurdere om den henviste saken gjelder spørsmål som omfattes av handelsdepartementets myndighetsområde, vurdere om det vil være nyttig med opplysningskampanjer rettet mot forbrukere og virksomheter samt eventuelt innlede en håndhevingsprosedyre.

FTC forplikter seg også til å utveksle informasjon om henviste saker med henvisende håndhevingsmyndigheter, herunder om status for de henviste sakene i henhold til lover og begrensninger om fortrolighet . I den grad det er mulig ut fra antall og type henviste saker som mottas, vil informasjonen omfatte en vurdering av de henviste sakene, herunder en beskrivelse av de viktigste punktene og eventuelle tiltak som er truffet for å håndtere lovovertredelser som faller inn under FTCs myndighet. FTC vil også gi henvisende myndighet tilbakemelding om typen henviste saker som er mottatt, for å gjøre innsatsen mot ulovlig atferd mer effektiv. Dersom en henvisende håndhevingsmyndighet ønsker informasjon om statusen for en bestemt henvist sak

([1]) Se FTC v. Karnani, No 2:09-cv-05276 (C.D. Cal. 20. mai 2011) (stipulert endelig kjennelse), tilgjengelig på 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, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9. juni 2011).

([2]) Brev fra Ken Hyatt, fungerende statssekretær for internasjonal handel, International Trade Administration, til Věra Jourová, kommissær for justis, forbrukersaker og likestilling.

for selv å kunne innlede en håndhevingsprosedyre, vil FTC i sitt svar ta hensyn til antall henviste saker som er under vurdering, samt krav til fortrolighet og andre lovfestede krav.

FTC vil også samarbeide tett med personvernmyndighetene i EU for å yte bistand i forbindelse med håndheving. I relevante tilfeller kan dette omfatte informasjonsutveksling og etterforskningsbistand i henhold til U.S. SAFE WEB Act, som tillater at FTC bistår utenlandske rettshåndhevende organer når det utenlandske organet håndhever lover som forbyr praksis som i hovedsak tilsvarer praksis som er forbudt i de lovene som FTC håndhever([1]). Som en del av denne bistanden kan FTC utveksle informasjon innhentet i forbindelse med en FTC-undersøkelse, innlede en obligatorisk prosedyre på vegne av personvern-myndigheten i EU som foretar sin egen undersøkelse, og innhente muntlige vitneforklaringer fra vitner eller innklagede i forbindelse med personvernmyndighetens håndhevingsprosedyre, forutsatt at kravene i U.S. SAFE WEB Act overholdes. FTC bruker denne myndigheten jevnlig til å bistå andre myndigheter rundt om i verden i saker om personvern og forbrukervern([2]).

I tillegg til å prioritere Privacy Shield-relaterte saker som henvises fra EU-medlemsstater og selvreguleringsorganisasjoner på personvernområdet([3]), vil FTC på eget initiativ og i relevant omfang undersøke mulige overtredelser av rammeverket ved bruk av en rekke verktøyer.

FTC har i mer enn ti år hatt et robust program for å undersøke aspekter knyttet til personvern og sikkerhet i forbindelse med handelsorganisasjoner. Som en del av disse undersøkelsene har FTC rutinemessig undersøkt om den aktuelle enheten har avgitt erklæringer knyttet til «trygg havn»-ordningen. Dersom enheten har avgitt slike erklæringer og undersøkelsen avdekket en åpenbar overtredelse av «trygg havn»-prinsippene for personvern, har FTC tatt med påstander om overtredelse av «trygg havn»-ordningen i sine håndhevingstiltak. Vi vil fortsette å bruke denne proaktive strategien i forbindelse med det nye rammeverket. Det skal understrekes at FTC foretar langt flere undersøkelser enn de som fører til offentlige håndhevingstiltak. Mange av FTCs undersøkelser avsluttes dersom personalet ikke kan påvise en åpenbar lovovertredelse. Ettersom FTCs undersøkelser ikke er offentlige og dessuten fortrolige, skjer det ofte at det ikke offentliggjøres at en undersøkelse avsluttes.

De nesten 40 håndhevingstiltakene truffet av FTC vedrørende «trygg havn»-ordningen vitner om FTCs fokus på å håndheve grensekryssende personvernprogrammer på en proaktiv måte. FTC vil søke etter potensielle overtredelser av rammeverket som ledd i personvern- og sikkerhetsundersøkelsene vi jevnlig foretar.

III. HÅNDTERING AV FALSKE ELLER VILLEDENDE PÅSTANDER OM DELTAKELSE I PRIVACY SHIELD-ORDNINGEN

Som nevnt ovenfor vil FTC treffe tiltak mot enheter som feilaktig påstår at de deltar i ordningen. FTC vil prioritere saker henvist fra det amerikanske handelsdepartementet angående organisasjoner som ifølge departementet feilaktig påstår at de deltar i ordningen, eller bruker ordningens sertifiseringsmerke uten tillatelse.

Vi understreker videre at dersom en organisasjon i sitt personvernprogram erklærer at den overholder Privacy Shield-prinsippene, vil det faktum at den ikke er eller ikke lenger er registrert ved handelsdepartementet, i seg selv ikke frita organisasjonen fra FTCs håndheving av de aktuelle forpliktelsene i henhold til ordningen.

([1]) Ved vurderingen av om FTC skal utøve sin myndighet i henhold til U.S. SAFE WEB Act, tar FTC bl.a. hensyn til det følgende: «A) Om det anmodende byrået har samtykket i å yte eller vil yte gjensidig bistand til FTC, B) om en overholdelse av anmodningen vil være til skade for De forente staters allmenne interesse og C) om det anmodende byråets undersøkelses- eller håndhevingsprosedyrer gjelder atferd eller praksis som forårsaker eller kan forårsake skade på et betydelig antall personer.» 15 U.S.C. § 46 (j) (3). Denne myndigheten får ikke anvendelse på håndheving av konkurranselover.

([2]) I regnskapsårene 2012–2015 brukte FTC f.eks. sin myndighet i henhold til U.S. SAFE WEB Act til å utveksle informasjon som svar på nærmere 60 anmodninger fra utenlandske organer, og utstedte nærmere 60 anmodninger om sivilrettslig granskning (tilsvarende administrative pålegg) for å bistå i 25 utenlandske undersøkelser.

([3]) Selv om FTC ikke løser eller megler i klager fra individuelle forbrukere, bekrefter FTC at de vil prioritere Privacy Shield-relaterte saker som henvises fra personvernmyndigheter i EU. FTC bruker i tillegg klager i sin Consumer Sentinel-database, som en rekke andre rettshåndhevende organer har tilgang til, til å identifisere trender, fastsette prioriteringer for håndhevingen og identifisere mulige mål som skal undersøkes. Privatpersoner i EU kan inngi klager til FTC via det samme klagesystemet som det amerikanske borgere bruker: www.ftc.gov/complaint. Når det gjelder individuelle Privacy Shield-relaterte klager, kan det imidlertid være mest hensiktsmessig for privatpersoner i EU å inngi klager til personvernmyndigheten i egen medlemsstat eller til et alternativt tvisteløsningsorgan.

IV. OVERVÅKING AV AVGJØRELSER

FTC bekrefter også at FTC vil overvåke håndhevingsavgjørelser for å sikre at Privacy Shield-rammeverket overholdes.

Vi vil stille krav om at rammeverket overholdes gjennom en rekke relevante forbudsbestemmelser i framtidige avgjørelser fra FTC knyttet til rammeverket. Dette omfatter forbud mot å oppgi uriktige opplysninger om rammeverket og andre personvern-programmer når disse ligger til grunn for den underliggende FTC-saken.

FTCs saker som gjelder håndheving av den opprinnelige «trygg havn»-ordningen, har vært lærerike. I de 36 sakene om falske eller villende påstander om «trygg havn»-sertifisering forbyr hver avgjørelse den saksøkte å avgi feilaktige opplysninger om vedkommendes deltakelse i «trygg havn»-ordningen eller andre personvern- eller sikkerhetsprogrammer, og krever at selskapet legger fram overholdelsesrapporter for FTC. I saker om overtredelse av «trygg havn»-prinsippene for personvern er selskaper blitt pålagt å gjennomføre omfattende personvernprogrammer og få vurdert disse programmene av uavhengige tredjeparter annethvert år i 20 år samt legge fram vurderingene for FTC.

Overtredelse av FTCs forvaltningsavgjørelser kan føre til idømming av sivilrettslige sanksjoner på opptil 16 000 USD per overtredelse eller 16 000 USD per dag dersom overtredelsen fortsetter([1]), noe som kan beløpe seg til flere millioner dollar dersom praksisen berører mange forbrukere. Enhver forlikavgjørelse inneholder også bestemmelser om rapportering og overholdelse. Enheter som omfattes av avgjørelser, skal oppbevare dokumenter som viser at de overholder prinsippene, i et nærmere bestemt antall år. Avgjørelsene skal også formidles til ansatte med ansvar for å overholde avgjørelser.

FTC foretar en systematisk overvåking av at «trygg havn»-avgjørelser overholdes, som med alle sine avgjørelser. FTC tar håndheving av sine avgjørelser om personvern og datasikkerhet alvorlig og treffer tiltak for å håndheve dem dersom det er nødvendig. Som nevnt ovenfor betalte Google f.eks. en bot på 22,5 millioner USD som følge av påstander om at selskapet ikke hadde overholdt FTCs avgjørelse vedrørende selskapet. Det er viktig å understreke at FTCs avgjørelser vil fortsette å beskytte alle forbrukere over hele verden som er i kontakt med en virksomhet, ikke bare forbrukere som har inngitt klager.

FTC vil fortsette å føre en nettbasert liste over selskaper som omfattes av avgjørelser truffet i forbindelse med håndheving av både «trygg havn»-ordningen og det nye Privacy Shield-rammeverket([2]). I henhold til Privacy Shield-prinsippene kreves det nå at selskaper som blir gjenstand for en avgjørelse fra FTC eller en rettsavgjørelse på grunn av manglende overholdelse av prinsippene, skal offentliggjøre alle relevante rammeverkrelaterte avsnitt i overholdelses- eller vurderingsrapporter som legges fram for FTC, i den grad dette er forenlig med lover om og regler for fortrolighet.

V. SAMARBEID MED PERSONVERNMYNDIGHETER I EU

FTC anerkjenner at personvernmyndigheter i EU spiller en viktig rolle med hensyn til å sikre overholdelse av rammeverket og oppmuntrer til økt samråd og samarbeid på dette området. I tillegg til samråd med henvisende personvernmyndigheter om saksspesifikke spørsmål vil FTC delta i regelmessige møter med utpekte representanter fra artikkel 29-arbeidsgruppen med henblikk på en generell drøfting av hvordan samarbeidet om håndheving av rammeverket kan bedres. Sammen med handelsdepartementet, Europakommisjonen og representanter for artikkel 29-arbeidsgruppen vil FTC også delta i den årlige gjennomgåelsen av rammeverket for å drøfte gjennomføringen av det.

FTC oppmuntrer også til utvikling av verktøyer som vil øke samarbeidet om håndheving av rammeverket med personvernmyndigheter i EU samt andre personvernmyndigheter rundt om i verden. Sammen med partnere med ansvar for håndheving i Den europeiske union og rundt om i verden lanserte FTC i fjor et varslingssystem innenfor rammen av Global Privacy Enforcement Network («GPEN») med henblikk på å utveksle informasjon om undersøkelser og fremme samordning av håndhevingsarbeidet. Dette GPEN-varslingsverktøyet kan være særdeles nyttig i forbindelse med Privacy Shield-rammeverket. FTC og personvernmyndigheter i EU kan bruke det til samordning av rammeverket og andre undersøkelser på området personvern, herunder som et utgangspunkt for å utveksle informasjon for å sikre et samordnet og mer effektivt personvern for

([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.

forbrukerne. Vi ser fram til å videreføre samarbeidet med deltakende myndigheter i EU om en mer generell anvendelse av GPEN-varslingssystemet og å utvikle andre verktøyer for å bedre samarbeidet om håndheving i saker om personvern, herunder saker som omfattes av rammeverket.

FTC er glade over å kunne bekrefte sin forpliktelse om å håndheve det nye Privacy Shield-rammeverket. Vi ser også fram til å fortsette samarbeidet med våre kolleger i EU om vern av forbrukernes personopplysninger på begge sider av Atlanteren.

Vennlig hilsen

Edith Ramirez

Leder

———

Tillegg A

Konteksten for rammeverket for Privacy Shield-avtalen mellom EU og De forente stater: En oversikt over rammene for personvern og sikkerhet i De forente stater

Det vernet som rammeverket for Privacy Shield-avtalen mellom EU og De forente stater («rammeverket») gir, er en del av det omfattende vernet av personopplysninger som det amerikanske rettssystemet som helhet sikrer. For det første har De forente staters Federal Trade Commission («FTC») et robust program for personvern og datasikkerhet i forbindelse med amerikansk handelspraksis som beskytter forbrukere over hele verden. For det andre har det skjedd en betydelig utvikling med hensyn til forbrukernes personvern og sikkerhet i De forente stater siden 2000 da den opprinnelige «trygg havn»-ordningen mellom EU og De forente stater ble vedtatt. Siden da er det vedtatt en rekke lover om personvern og sikkerhet på føderalt plan og delstatsplan, og antall offentlige og private tvister for å håndheve personvernrettigheter har økt betraktelig. De forente staters omfattende rettslige vern med hensyn til forbrukernes personvern og sikkerhet som gjelder amerikansk handelspraksis, utfyller det vernet som det nye rammeverket gir privatpersoner i EU.

I. FTCs GENERELLE PROGRAM FOR HÅNDHEVING PÅ OMRÅDET PERSONVERN OG SIKKERHET

FTC er De forente staters ledende forbrukervernbyrå med fokus på personvern i handelssektoren. FTC har myndighet til å anlegge sak mot urimelig og villedende atferd eller praksis som krenker forbrukernes personvern, samt til å håndheve mer målrettede personvernlover som har som formål å verne visse finansielle opplysninger og helseopplysninger, opplysninger om barn og opplysninger som brukes til å treffe visse avgjørelser om klassifisering av forbrukere.

FTC har en unik erfaring når det gjelder å ivareta forbrukernes personvern. FTCs håndhevingstiltak har gjort det mulig å håndtere ulovlig praksis både på og utenfor internett. FTC har f.eks. truffet håndhevingstiltak mot velkjente selskaper som Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC og Snapchat samt mindre kjente selskaper. FTC har anlagt sak mot virksomheter på grunnlag av påstander om at de har sendt søppelpost til forbrukere, installert spionprogramvare på datamaskiner, unnlatt å sikre forbrukernes personopplysninger, sporet forbrukere ulovlig på internett, krenket barns personvern, ulovlig har samlet inn opplysninger på forbrukernes mobile enheter og unnlatt å sikre nettilkoplede enheter som brukes til lagring av personopplysninger. De avgjørelsene som er truffet i disse sakene, har vanligvis medført løpende overvåking fra FTCs side i en periode på 20 år, hindret ytterligere lovovertredelser og pålagt virksomheter betydelige økonomiske sanksjoner i tilfelle manglende overholdelse av avgjørelsen([1]). Det er viktig å understreke at FTCs avgjørelser ikke bare verner de som har klaget over et problem, men alle forbrukere som vil ha med virksomheten å gjøre i framtiden. I en internasjonal sammenheng har FTC myndighet til å verne forbrukere i hele verden mot praksis som finner sted i De forente stater([2]).

Hittil har FTC anlagt over 130 saker om søppelpost og spionprogramvare, over 120 saker om brudd på «Do Not Call»-ordningen i forbindelse med telefonmarkedsføring, over 100 saker i forbindelse med Fair Credit Reporting Act, nesten 60 saker om datasikkerhet, mer enn 50 generelle saker om personvern, nesten 30 saker om brudd på Gramm-Leach-Bliley Act og over 20 saker om håndheving av Children's Online Privacy Protection Act («COPPA»)([3]). I tillegg til disse sakene har FTC også utstedt og offentliggjort advarselsbrev([4]).

([1]) Enhver enhet som ikke retter seg etter en FTC-avgjørelse, kan ilegges en bot på opptil 16 000 USD per overtredelse eller 16 000 USD per dag dersom overtredelsen fortsetter. Se 15 U.S.C. § 45 (l); 16 C.F.R. § 1.98 (c).

([2]) Kongressen har uttrykkelig bekreftet FTCs myndighet til å gjøre bruk av rettsmidler, herunder restitusjon, i forbindelse med enhver atferd eller praksis som involverer utenlandsk handel, og som 1) forårsaker eller vil kunne forårsake skade i De forente stater som med rimelighet kan forutses, eller 2) omfatter en konkret atferd i De forente stater. Se 15 U.S.C. § 45 (a) (4).

([3]) I FTCs saker om personvern og datasikkerhet er det i visse tilfeller blitt hevdet at et selskap har vært involvert i både urimelig eller villedende praksis; disse sakene omfatter noen ganger også påståtte overtredelser av flere lover, f.eks. Fair Credit Reporting Act, Gramm-Leach-Bliley Act og COPPA.

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

Som en del av sin historisk sett sterke håndheving på området personvern har FTC også regelmessig undersøkt eventuelle overtredelser av «trygg havn»-programmet. Siden «trygg havn»-programmet ble vedtatt, har FTC på eget initiativ foretatt en rekke undersøkelser av overholdelsen av programmet og har ført 39 saker mot amerikanske selskaper for brudd på «trygg havn»-programmet. FTC vil videreføre denne proaktive strategien ved å prioritere håndhevingen av det nye rammeverket.

II. IVARETAKELSE AV FORBRUKERNES PERSONVERN PÅ FØDERALT PLAN OG DELSTATSPLAN

Oversikten over håndhevingen av «trygg havn»-ordningen som finnes som et vedlegg til Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå, inneholder en oppsummering av mange av de føderale og delstatlige personvernlovene som gjaldt da «trygg havn»-programmet ble vedtatt i 2000([1]). På det daværende tidspunkt ble innsamling og bruk av personopplysninger til kommersielle formål regulert av en rekke føderale lover som foruten avsnitt 5 i FTC Act omfattet 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. En rekke delstater hadde også tilsvarende lover på disse områdene.

Siden 2000 har det skjedd mye på både føderalt plan og delstatsplan som har styrket forbrukernes personvern([2]). På føderalt plan endret FTC f.eks. COPPA-regelen i 2013 for å styrke vernet av barns personopplysninger. FTC har også utstedt to regler som gjennomfører Gramm-Leach-Bliley Act – Privacy Rule og Safeguards Rule – som pålegger finansinstitusjoner([3]) å offentliggjøre sin praksis for utveksling av informasjon og å gjennomføre et omfattende informasjonssikkerhetsprogram for å verne forbrukeropplysninger([4]). Fair and Accurate Credit Transactions Act («FACTA»), vedtatt i 2003, supplerer også den mangeårige amerikanske kredittlovgivningen med det formål å fastsette krav til maskering, utveksling og sletting av visse sensitive finansielle opplysninger. FTC har vedtatt en rekke regler i henhold til FACTA om bl.a. forbrukernes rett til en gratis årlig kredittrapport, krav til sikker sletting av opplysninger i forbrukerrapporter, forbrukernes rett til reservere seg mot å motta visse tilbud om kreditt og forsikring, forbrukernes rett til å nekte bruk av opplysninger som leveres av et tilknyttet selskap, til å markedsføre dets produkter og tjenester, og krav til at finansinstitusjoner og kreditorer skal gjennomføre programmer for å avdekke og forebygge identitetstyveri([5]). Reglene vedtatt i henhold til Health Insurance Portability and Accountability Act ble dessuten revidert i 2013, og det ble innført nye garantier for vern av og sikkerhet for personopplysninger som gjelder helse([6]). Regler som beskytter forbrukere mot uønskede oppringninger med telefonmarkedsføring, automatiske oppringninger og søppelpost, har også trådt i kraft. Kongressen har dessuten vedtatt lover som krever at visse selskaper som samler inn helseopplysninger, skal underrette forbrukerne dersom det skjer en overtredelse([7]).

Delstatene har også vært svært aktive når det gjelder å vedta lover knyttet til personvern og sikkerhet. Siden 2000 har 47 delstater, District of Columbia, Guam, Puerto Rico og De amerikanske Jomfruøyer vedtatt lover som krever at virksomheter

([1]) Se U.S. Dep't of Commerce, Safe Harbor Enforcement Overview (https://build.export.gov/main/safeharbor/eu/eg_main_018476).

([2]) Se Daniel J. Solove & Paul Schwartz, Information Privacy Law (femte utgave 2015) for å få et mer omfattende sammendrag av det rettslige vernet i De forente stater.

([3]) I Gramm-Leach-Bliley Act defineres finansinstitusjoner svært bredt og omfatter alle virksomheter som «i vesentlig grad beskjeftiger seg med» levering av finansielle produkter eller tjenester. Dette omfatter f.eks. sjekkinnløsningsvirksomheter, «payday lenders» (lån fram til og som innløses neste lønningsdag), boliglånmeglere, långivere som ikke er banker, takstmenn for personlige eiendeler eller fast eiendom, og selskaper som utarbeider skattemeldinger for næringsdrivende.

([4]) I forbindelse med Consumer Financial Protection Act fra 2010 («CFPA»), Title X of Pub. L. 111-203, 124 Stat. 1955 (21. juli 2010) (også kjent som «Dodd-Frank Wall Street Reform and Consumer Protection Act») ble den største delen av FTCs reguleringsmyndighet i henhold til Gramm-Leach-Bliley Act overført til Consumer Financial Protection Bureau («CFPB»). FTC har fortsatt håndhevingsmyndighet i henhold til Gramm-Leach- Bliley Act samt reguleringsmyndighet for Safeguards Rule og begrenset reguleringsmyndighet i henhold til Privacy Rule når det gjelder bilforhandlere.

([5]) I henhold til CFPA deler FTC sin håndhevingsrolle i henhold til FCRA med CFPB, men en stor del av reguleringsmyndigheten er overført til CFPB (med unntak av Red Flags Rule og Disposal Rule).

([6]) Se 45 C.F.R. punkt 160, 162, 164.

([7]) Se f.eks. American Recovery & Reinvestment Act fra 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. punkt 318.

skal underrette personer om brudd på sikkerheten for personopplysninger([1]). Minst 32 delstater og Puerto Rico har lover om sletting av opplysninger der det er innført krav om tilintetgjøring eller sletting av personopplysninger([2]). En rekke delstater har også vedtatt generelle lover om datasikkerhet. I tillegg har California vedtatt en rekke lover om personvern, herunder en lov som krever at selskaper skal ha personvernprogrammer og offentliggjøre sin praksis for ikke-sporing («Do Not Track»)([3]), en «Shine the Light»-lov som pålegger datameglere større åpenhet([4]), og en lov om en «sletteknapp» som gjør det mulig for mindreårige å be om å få slettet visse opplysninger fra sosiale medier([5]). Ved hjelp av disse lovene og annen myndighet har myndigheter på føderalt plan og delstatsplan ilagt selskaper som har unnlatt å sikre vern av forbrukernes personopplysninger, betydelige bøter([6]).

Søksmål anlagt av privatpersoner har også ført til dommer og forlik som har sikret forbrukerne ytterligere personvern og datasikkerhet. I 2015 samtykket Target f.eks. i å betale 10 millioner USD som en del av et forlik med kunder som hevdet at deres personlige finansielle opplysninger var blitt brakt i fare som følge av et omfattende brudd på opplysningssikkerheten. I 2013 samtykket AOL i å betale 5 millioner USD som en del av et forlik for å løse et gruppesøksmål på grunnlag av en påstand om utilstrekkelig anonymisering i forbindelse med offentliggjøring av søkespørringene til hundretusentalls AOL-medlemmer. En føderal domstol avgjorde også at Netflix skulle betale 9 millioner USD for angivelig å ha oppbevart leiehistorikk i strid med Video Privacy Protection Act fra 1988. Føderale domstoler i California godkjente to separate forlik med Facebook, det ene pålydende 20 millioner USD, det andre pålydende 9,5 millioner USD, vedrørende selskapets innsamling, bruk og utveksling av brukernes personopplysninger. I 2008 godkjente en delstatsdomstol i California et forlik pålydende 20 millioner USD med LensCrafters pga. ulovlig utlevering av forbrukernes helseopplysninger.

Kort sagt gir De forente stater et betydelig rettslig vern med hensyn til forbrukernes personvern og sikkerhet, noe som også framgår av dette sammendraget. Det nye Privacy Shield-rammeverket, som sikrer privatpersoner i EU omfattende garantier, vil inngå i en større sammenheng der forbrukernes personvern og sikkerhet fortsatt er en viktig prioritering.

———

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

([2]) NCSL, Data Disposal Laws (12. jan. 2016), tilgjengelig på 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 (17. feb. 2014), tilgjengelig på http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

VEDLEGG V

Brev fra Anthony Foxx, De forente staters transportminister

19. februar 2016

Kommissær Vera Jourová
Europakommisjonen
Rue de la Loi / Wetstraat 200
1049 Brussel
Belgia

Angående: Rammeverket for Privacy Shield-avtalen mellom EU og De forente stater

Kjære kommissær Jourová

De forente staters transportdepartement («departementet») er glad over muligheten til å beskrive sin rolle i håndhevingen av rammeverket for Privacy Shield-avtalen mellom EU og De forente stater. Dette rammeverket spiller en avgjørende rolle når det gjelder å fremme vern av personopplysninger som overføres i forbindelse med kommersielle transaksjoner i en stadig mer sammenkoplet verden. Det gjør det mulig for foretak å gjennomføre viktige transaksjoner i den globale økonomien og samtidig sikre et fortsatt sterkt vern av personopplysningene til forbrukere i EU.

Transportdepartementet forpliktet seg første gang offentlig til å håndheve «trygg havn»-ordningen i et brev til Europakommisjonen for over 15 år siden. I dette brevet forpliktet transportdepartementet seg til å håndheve «trygg havn»-prinsippene for personvern strengt. Transportdepartementet fortsetter å overholde denne forpliktelsen, noe som understrekes i dette brevet.

Transportdepartementet bekrefter på nytt sine forpliktelser på følgende sentrale områder: 1) Prioritering av undersøkelser av påståtte overtredelser av Privacy Shield-ordningen, 2) iverksetting av egnede håndhevingstiltak mot enheter som framsetter falske eller villedende påstander om Privacy Shield-sertifisering, og 3) overvåking og offentliggjøring av håndhevingsavgjørelser angående overtredelse av Privacy Shield-ordningen. Vi redegjør for hver av disse forpliktelsene og for den relevante bakgrunnen for transportdepartementets rolle når det gjelder å ivareta forbrukernes personvern og håndheve Privacy Shield-rammeverket.

I. BAKGRUNN

A. **Transportdepartementets myndighet på området personvern**

Departementet er sterkt opptatt av å sikre vern av opplysninger som forbrukere gir flyselskaper og billettagenter. Transportdepartementets myndighet til å treffe tiltak på dette området er hjemlet i 49 U.S.C. 41712, som forbyr transportører eller billettagenter å benytte «urimelige eller villedende praksis eller urimelige konkurransemetoder», som er eller kan være til skade for forbrukeren, ved salg av lufttransportytelser. Avsnitt 41712 er utformet etter avsnitt 5 i Federal Trade Commission (FTC) Act (15 U.S.C. 45). I henhold til vår tolkning forbyr vår lov om urimelig eller villedende praksis luftfartsselskaper eller billettagenter 1) å overtre vilkårene i sitt personvernprogram eller 2) å samle inn eller utlevere personopplysninger på en måte som strider mot den offentlige orden, er umoralsk eller medfører en betydelig skade for forbrukerne som ikke oppveies av andre fordeler. Vi tolker også avsnitt 41712 dithen at det er forbudt for transportører og billettagenter 1) å overtre enhver regel utstedt av departementet som identifiserer en spesifikk personvernpraksis som urimelig eller villedende, eller 2) å overtre Children's Online Privacy Protection Act (COPPA) eller FTCs regler som gjennomfører COPPA. I henhold til føderal rett er det bare transportdepartementet som har myndighet til å regulere luftfartsselskapenes personvernpraksis, og departementet deler myndighet med FTC når det gjelder billettagenters personvernpraksis ved salg av lufttransportytelser.

Når en transportør eller selger av lufttransportytelser offentlig forplikter seg til å overholde personvernprinsippene i Privacy Shield-rammeverket, kan departementet derfor benytte sin lovfestede myndighet i henhold til avsnitt 41712 for å sikre at disse prinsippene overholdes. Når en passasjer gir opplysninger til en transportør eller billettagent som har forpliktet seg til å overholde prinsippene for personvern i Privacy Shield-rammeverket, vil enhver manglende overholdelse av prinsippene fra transportørens eller billettagentens side derfor utgjøre en overtredelse av avsnitt 41712.

B. **Håndhevingspraksis**

Departementets Office of Aviation Enforcement and Proceedings (Aviation Enforcement Office) undersøker og anlegger saker i henhold til 49 U.S.C. 41712. Det håndhever det lovfestede forbudet i avsnitt 41712 mot urimelig og villedende praksis hovedsakelig gjennom forhandlinger, utarbeiding av forbud mot fortsatt virksomhet («cease and desist orders») og utkast til avgjørelser om sivilrettslige sanksjoner. Kontoret får primært kjennskap til potensielle overtredelser gjennom klager det mottar fra privatpersoner, reisebyråer, luftfartsselskaper og amerikanske og utenlandske offentlige organer. Forbrukere kan inngi personvernrelaterte klager på luftfartsselskaper og billettagenter via transportdepartementets nettsted([1]).

Dersom det ikke inngås et rimelig og egnet forlik i en sak, har Aviation Enforcement Office myndighet til å innlede en håndhevingsprosedyre med bevishøring for en av transportdepartementets forvaltningsdommere («administrative law judge» – ALJ). ALJ har myndighet til å utstede forbud mot fortsatt virksomhet («cease-and desist orders») og sivilrettslige sanksjoner. Overtredelser av avsnitt 41712 kan føre til utstedelse av forbud mot fortsatt virksomhet og ilegging av sivilrettslige sanksjoner på opptil 27 500 USD for hver overtredelse av avsnitt 41712.

Departementet har ikke myndighet til å tilkjenne skadeserstatning eller gi økonomisk godtgjøring til individuelle klagere. Departementet har imidlertid myndighet til å godkjenne forlik som inngås på bakgrunn av undersøkelser foretatt av Aviation Enforcement Office, og som er til direkte nytte for forbrukerne (f.eks. kontantbeløp, verdikuponger), som en erstatning for de pengebøtene som ellers skulle betales til den amerikanske regjering. Dette har skjedd før og kan skje igjen i forbindelse med Privacy Shield-prinsippene når omstendighetene taler for det. Dersom et luftfartsselskap gjentatte ganger overtrer avsnitt 41712, vil det også oppstå tvil om selskapets evne til i det hele tatt å overholde loven, noe som i ekstreme tilfeller kan medføre at det blir ansett som uegnet til å drive virksomhet, og dermed mister sin tillatelse til det.

Hittil har transportdepartementet mottatt relativt få klager med påstand om at billettagenter eller luftfartsselskaper har krenket personvernet. Når det skjer, undersøkes klagene i henhold til prinsippene angitt ovenfor.

C. **Transportdepartementets rettslige vern som forbrukere i EU nyter godt av**

I henhold til avsnitt 41712 får forbudet mot urimelig eller villedende praksis innen lufttransport eller salg av lufttransportytelser anvendelse på amerikanske og utenlandske transportører og billettagenter. Transportdepartementet griper ofte inn overfor amerikanske og utenlandske luftfartsselskapers praksis som berører både utenlandske og amerikanske forbrukere, på det grunnlag at luftfartsselskapets praksis ble utøvd i forbindelse med transport til eller fra De forente stater. Transportdepartementet benytter og vil fortsatt benytte alle tilgjengelige rettsmidler for å beskytte både utenlandske og amerikanske forbrukere mot regulerte foretaks urimelige eller villedende praksis innen lufttransport.

Når det gjelder luftfartsselskaper, håndhever transportdepartementet dessuten andre målrettede lover hvis bestemmelser om vern også får anvendelse på ikke-amerikanske forbrukere, f.eks. COPPA. I henhold til COPPA skal operatører av nettsteder og nettjenester rettet mot barn eller nettsteder rettet mot allmennheten som bevisst samler inn personopplysninger fra barn under 13 år, blant annet informere foreldrene og innhente et kontrollerbart samtykke fra foreldrene. USA-baserte nettsteder og -tjenester som omfattes av COPPA, og som samler inn personopplysninger fra utenlandske barn, skal overholde COPPA. Utenlandske nettsteder og nettjenester må også overholde COPPA dersom de er rettet mot barn i De forente stater, eller dersom de bevisst samler inn personopplysninger fra barn i De forente stater. Transportdepartementet har myndighet til å treffe håndhevingstiltak overfor amerikanske eller utenlandske luftfartsselskaper som opererer i De forente stater og overtrer COPPA.

II. HÅNDHEVING AV PRIVACY SHIELD-RAMMEVERKET

Dersom et luftfartsselskap eller en billettagent velger å delta i Privacy Shield-ordningen og departementet mottar en klage med påstand om at nevnte luftfartsselskap eller billettagent ikke overholder rammeverket, vil departementet treffe følgende tiltak for å håndheve rammeverket strengt.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Prioriterte undersøkelser av påståtte overtredelser**

Departementets Aviation Enforcement Office vil undersøke enhver klage på påståtte overtredelser av Privacy Shield-ordningen (herunder klager mottatt fra personvernmyndigheter i EU) og treffe håndhevingstiltak dersom det foreligger bevis på overtredelsen. Aviation Enforcement Office vil dessuten samarbeide med FTC og det amerikanske handelsdepartementet og prioritere påstander om at de regulerte foretakene ikke overholder de forpliktelsene på området personvern som de har inngått som en del av Privacy Shield-ordningen.

Ved mottak av en påstand om manglende overholdelse av Privacy Shield-rammeverket kan departementets Aviation Enforcement Office treffe en rekke tiltak som ledd i sin undersøkelse. Det kan f.eks. gjennomgå billettagentens eller luftfartsselskapets personvernprogrammer, innhente ytterligere informasjon fra billettagenten eller luftfartsselskapet eller fra tredjeparter, følge opp saken overfor den henvisende instansen og vurdere om overtredelsene følger et mønster, eller om et betydelig antall forbrukere er berørt. I tillegg vil det vurdere om saken gjelder spørsmål som omfattes av handelsdepartementets eller FTCs myndighetsområde, om det vil være nyttig å iverksette opplysningskampanjer rettet mot forbrukere og virksomheter samt eventuelt innlede en håndhevingsprosedyre.

Dersom departementet får kjennskap til at billettagenter kan ha overtrådt Privacy Shield-ordningen, vil departementet samordne saken med FTC. Vi vil også underrette FTC og handelsdepartementet om utfallet av ethvert Privacy Shield-relatert håndhevingstiltak.

B. **Håndtering av falske eller villedende påstander om deltakelse**

Departementet vil fortsatt undersøke overtredelser av Privacy Shield-prinsippene, herunder falske eller villedende påstander om deltakelse i Privacy Shield-ordningen. Vi vil prioritere henvisninger fra handelsdepartementet angående organisasjoner som ifølge departementet feilaktig påstår at de deltar i Privacy Shield-ordningen eller bruker Privacy Shield-sertifiseringsmerket uten tillatelse.

Vi understreker i tillegg at dersom en organisasjon i sitt personvernprogram lover at den overholder de vesentlige Privacy Shield-prinsippene, vil det faktum at den ikke er eller ikke lenger er registrert ved handelsdepartementet, i seg selv ikke være nok til å hindre at transportdepartementet kan kreve at forpliktelsene overholdes.

C. **Overvåking og offentliggjøring av håndhevingsavgjørelser angående overtredelse av Privacy Shield-ordningen**

Departementets Aviation Enforcement Office vil også fortsatt overvåke håndhevingsavgjørelser for å sikre at Privacy Shield-ordningen overholdes. Dersom kontoret utsteder en avgjørelse som pålegger et luftfartsselskap eller en billettagent å avstå fra framtidige overtredelser av Privacy Shield-ordningen og avsnitt 41712, vil det kontrollere at foretaket overholder avgjørelsens bestemmelse om dette. Kontoret vil dessuten sørge for at avgjørelser som utstedes i forbindelse med Privacy Shield-saker, er tilgjengelige på kontorets nettsted.

Vi ser fram til et fortsatt samarbeid med våre føderale partnere og berørte parter i EU om spørsmål som gjelder Privacy Shield-ordningen.

Jeg håper denne informasjonen vil være til nytte. Jeg står naturligvis til rådighet dersom De har spørsmål eller ønsker ytterligere opplysninger.

Vennlig hilsen

Anthony R. Foxx

Transportminister

———

VEDLEGG VI

Brev fra Robert Litt, General Counsel

Office of the Director of National Intelligence

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

Kjære Justin Antonipillai og Ted Dean

I de siste to og et halvt år har De forente stater i forbindelse med forhandlingene om Privacy Shield-avtalen mellom EU og De forente stater framlagt omfattende informasjon om det amerikanske etterretningssamfunnets signaletterretningsaktiviteter. Dette har omfattet informasjon om gjeldende rettslige ramme, tilsynet på flere plan med disse aktivitetene, den omfattende åpenheten rundt disse aktivitetene samt de generelle tiltakene for å ivareta personvernet og de borgerlige frihetsrettighetene for å gjøre det lettere for Europakommisjonen å vurdere om dette vernet er tilstrekkelig, ettersom de gjelder unntaket for nasjonal sikkerhet i Privacy Shield-prinsippene. Dette dokumentet inneholder en oppsummering av informasjonen som er framlagt.

I. PPD-28 OG DE FORENTE STATERS SIGNALETTERRETNINGSAKTIVITETER

Det amerikanske etterretningssamfunnet samler inn utenlandsetterretning på en nøye kontrollert måte og i nøye samsvar med amerikansk rett; virksomheten er underlagt tilsyn på flere nivåer, og det fokuseres på viktige prioriteringer på området utenlandsetterretning og nasjonal sikkerhet. Det amerikanske etterretningssamfunnets innsamling av signaletterretning reguleres av en mosaikk av lover og retningslinjer, herunder den amerikanske grunnloven, Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 *et seq.*) (FISA), Executive Order 12333 og dens gjennomføringsprosedyrer, presidentdirektiver og en rekke prosedyrer og retningslinjer godkjent av FISA-domstolen og den amerikanske justisministeren som inneholder ytterligere regler som begrenser innsamling, lagring, bruk og spredning av utenlandsetterretningsinformasjon([1]).

a. **PPD 28 – oversikt**

I januar 2014 holdt president Obama en tale der han redegjorde for forskjellige reformer av De forente staters signal-etterretningsaktiviteter. Presidenten utstedte også Presidential Policy Directive 28 (PPD-28) om disse aktivitetene([2]). Presidenten understreket at De forente staters signaletterretningsaktiviteter bidrar til å sikre ikke bare vårt land og vår frihet, men også sikkerheten og friheten til andre land, herunder EU-medlemsstatene, som benytter informasjon innhentet av amerikanske etterretningsbyråer til å beskytte egne borgere.

I PPD-28 fastsettes en rekke prinsipper og krav som gjelder for alle amerikanske signaletterretningsaktiviteter og for alle mennesker, uavhengig av deres statsborgerskap eller bosted. Det stilles særlig bestemte krav til framgangsmåter for innsamling, lagring og spredning av personopplysninger om ikke-amerikanske personer innhentet innenfor rammen av De forente staters signaletterretningsaktiviteter. Det redegjøres nærmere for disse kravene nedenfor, men her følger en kort oppsummering:

— I PPD understrekes det at De forente staters innsamling av signaletterretning bare skjer i henhold til de metodene som er godkjent ved lov, presidentordrer («executive orders») eller andre presidentdirektiver («presidential directives»).

([1]) Ytterligere informasjon om De forente staters utenlandsetterretningsaktiviteter er lagt ut på internett og er offentlig tilgjengelig via nettstedet IC on the Record (www.icontherecord.tumblr.com), ODNIs offentlige nettsted som har som mål å fremme større offentlig åpenhet om regjeringens etterretningsaktiviteter.

([2]) Tilgjengelig på https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— I PPD fastsettes framgangsmåter for å sikre at signaletterretningsaktiviteter bare gjennomføres i forbindelse med berettigede og godkjente formål knyttet til nasjonal sikkerhet.

— I henhold til PPD skal hensynet til personvern og borgerlige frihetsrettigheter integreres i planleggingen av innsamling av signaletterretning. De forente stater samler ikke inn etterretning med det formål å undertrykke eller hindre kritikk eller uenighet, forskjellsbehandle personer på grunnlag av deres etniske opprinnelse, rase, kjønn, seksuelle legning eller religion eller å gi amerikanske selskaper og næringssektorer forretningsmessige konkurransefortrinn.

— I henhold til PPD skal innsamlingen av signaletterretning være så målrettet som mulig, og masseinnsamlet signaletterretning kan bare brukes til spesifikt angitte formål.

— I henhold til PPD skal etterretningssamfunnet innføre prosedyrer som i «rimelig grad er utformet for å minimere spredning og lagring av personopplysninger som er samlet inn via signaletterretningsaktiviteter», og særlig utvide en del av det vernet som amerikanske personers personopplysninger omfattes av, til også å gjelde ikke-amerikanske personers personopplysninger.

— Byråenes prosedyrer for gjennomføring av PPD-28 er blitt vedtatt og offentliggjort.

Det står klart at prosedyrene og vernetiltakene fastsatt her kan anvendes på Privacy Shield-ordningen. Når opplysninger er blitt overført til foretak i De forente stater innenfor rammen av Privacy Shield-ordningen, eller på en hvilken som helst annen måte, kan amerikanske etterretningsbyråer anmode om å få tilgang til nevnte opplysninger fra disse foretakene bare dersom anmodningene er i samsvar med FISA eller inngis i henhold til en av de lovfestede bestemmelsene om det nasjonale sikkerhetsbrevet (NSL), som drøftes nedenfor([1]). Uten å bekrefte eller avkrefte medierapporter der det hevdes at det amerikanske etterretningssamfunnet samler inn opplysninger fra transatlantiske kabler mens opplysningene overføres til De forente stater, vil det amerikanske etterretningssamfunnet, dersom det skulle samle inn opplysninger fra transatlantiske kabler, være underlagt de begrensningene og garantiene som er fastsatt her, herunder kravene i PPD-28.

b. **Begrensninger for innsamling**

I PPD-28 er det fastsatt en rekke viktige generelle prinsipper for innsamling av signaletterretning:

— Innsamling av signaletterretning skal være hjemlet i lov eller godkjent av presidenten, og skal gjennomføres i samsvar med grunnloven og nasjonal rett.

— Hensynet til personvern og borgerlige frihetsrettigheter skal integreres i planleggingen av signaletterretningsaktiviteter.

— Signaletterretning vil bli samlet inn bare når det foreligger et gyldig utenlandsetterretnings- eller kontraspionasjeformål.

— De forente stater vil ikke samle inn signaletterretning med det formål å undertrykke eller hindre kritikk eller uenighet.

— De forente stater vil ikke samle inn signaletterretning med det formål å forskjellsbehandle mennesker basert på deres etniske opprinnelse, rase, kjønn, seksuelle legning eller religion.

— De forente vil ikke samle inn signaletterretning med det formål å gi amerikanske selskaper og næringssektorer et forretningsmessig konkurransefortrinn.

— Amerikanske signaletterretningsaktiviteter skal *alltid* være så målrettede som mulig, og andre tilgjengelige informasjonskilder skal tas i betraktning. Dette betyr blant annet at når det er praktisk mulig, skal innsamlingen av signaletterretning målrettes istedenfor at det foretas masseinnsamling.

Kravet om at signaletterretningsaktiviteter skal være «så målrettede som mulig» gjelder måten signaletterretningen samles inn på, samt hva som rent faktisk samles inn. Når det amerikanske etterretningssamfunnet f.eks. skal bestemme om

([1]) Rettshåndhevings- eller reguleringsorganer kan anmode om opplysninger fra selskaper for etterforskningsformål i De forente stater i henhold til andre strafferettslige, sivilrettslige og regulerende myndigheter som ikke omhandles i dette dokumentet, som bare gjelder nasjonale sikkerhetsmyndigheter.

signaletterretning skal samles inn, skal det ta høyde for annen tilgjengelig informasjon, herunder diplomatiske eller offentlige kilder, og prioritere innsamling ved bruk av disse metodene når det er hensiktsmessig og mulig. I retningslinjene til enheter innen etterretningssamfunnet bør det stilles krav om at innsamlingen, når det er praktisk mulig, bør fokusere på spesifikke utenlandske etterretningsmål eller -emner ved bruk av diskriminanter (f.eks. bestemte fasiliteter, utvalgskriterier og identifikatorer).

Det er viktig å se på informasjonen framlagt for Kommisjonen i et helhetsperspektiv. Avgjørelser om hva som er «mulig» eller «praktisk mulig» overlates ikke til den enkelte, men er underlagt retningslinjene som byråer har utstedt i henhold til PPD-28 – som er blitt offentliggjort – og de andre prosessene beskrevet der([1]). Som angitt i PPD-28 er masseinnsamling av signaletterretning innsamling som «av tekniske eller praktiske hensyn foretas uten bruk av diskriminanter (f.eks. spesifikke identifikatorer, utvalgskriterier osv.)». I denne forbindelse anerkjennes det i PPD-28 at enheter i etterretningssamfunnet i visse situasjoner må foreta masseinnsamling av signaletterretning for å identifisere nye eller framvoksende trusler og annen svært viktig informasjon knyttet til nasjonal sikkerhet som ofte er skjult i store og sammensatte moderne og globale kommunikasjonssystemer. Det anerkjennes også at masseinnsamling av signaletterretning vekker bekymring med hensyn til personvern og borgerlige frihetsrettigheter. Ved PPD-28 pålegges etterretningssamfunnet derfor å prioritere alternativer som gjør det mulig å foreta målrettet innsamling av signaletterretning istedenfor masseinnsamling. Når det er praktisk mulig, skal enheter i etterretningssamfunnet derfor foreta målrettet innsamling av signaletterretning istedenfor masseinnsamling([2]). Disse prinsippene sikrer at unntaket som gjelder masseinnsamling, ikke blir den alminnelige regelen.

Når det gjelder konseptet «rimelighet», er det et grunnleggende prinsipp i amerikansk rett. Det betyr at enheter innen etterretningssamfunnet ikke trenger å vedta teoretisk mulige tiltak, men at innsatsen for å verne berettigede interesser knyttet til personvern og borgerlige frihetsrettigheter skal stå i forhold til signaletterretningsaktivitetenes praktiske behov. Også her er byråenes retningslinjer gjort tilgjengelig og gir en forsikring om at begrepet «i rimelig grad er utformet for å minimere spredning og lagring av personopplysninger» ikke underminerer den alminnelige regelen.

I PPD-28 er det også fastsatt at masseinnsamlet signaletterretning bare kan brukes for seks spesifikke formål: Avdekke og nøytralisere visse aktiviteter som utøves av fremmede makter, terrorbekjempelse, hindre massespredning av kjernefysiske våpen, cybersikkerhet, avdekke og nøytralisere trusler mot De forente stater eller allierte væpnede styrker og bekjempe tverrnasjonale kriminelle trusler, herunder unndragelse av sanksjoner. Presidentens nasjonale sikkerhetsrådgiver (National Security Advisor) vil i samarbeid med direktøren for National Intelligence (DNI) hvert år gjennomgå denne tillatte bruken av masseinnsamlet signaletterretning for å undersøke om den bør endres. DNI vil i størst mulig grad gjøre denne listen offentlig, idet det tas hensyn til den nasjonale sikkerheten. Dette sikrer en viktig og gjennomsiktig begrensning i bruken av masseinnsamling av signaletterretning.

Enhetene i etterretningssamfunnet med ansvar for å gjennomføre PPD-28 har dessuten styrket eksisterende analysepraksis og -standarder for søk som gjelder ikke-vurdert signaletterretning([3]). Analytikerne skal strukturere sine søk eller andre søketermer og -teknikker for å sikre at de er egnet med henblikk på å identifisere etterretningsinformasjon som er relevant for en gyldig utenlandsetterretnings- eller rettshåndhevingsoppgave. I denne forbindelse skal enheter i etterretningssamfunnet fokusere forespørsler om personer på kategorier av signaletterretningsinformasjon som oppfyller et utenlandsetterretnings- eller rettshåndhevingskrav, for å hindre bruk av personopplysninger som ikke oppfyller slike krav.

Det er viktig å understreke at enhver masseinnsamling av internettkommunikasjon som De forente staters etterretningssamfunn foretar gjennom signaletterretning, bare omfatter en liten del av internett. Bruken av målrettede søk, som beskrevet ovenfor, sikrer at analytikere får seg forelagt bare de opplysningene som antas å ha en potensiell etterretningsverdi. Hensikten med disse begrensningene er å ivareta personvernet og de borgerlige frihetsrettighetene til alle personer, uavhengig av deres statsborgerskap eller bosted.

([1]) Tilgjengelig på www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Gjennom disse prosedyrene gjennomføres den målrettede overvåkningen som det redegjøres for i dette brevet, på en bestemt måte i de enkelte etterretningsenhetene.

([2]) For å nevne ett eksempel angis det i NSAs prosedyrer som gjennomfører PPD-28, at «når det er mulig, skal innsamlingen skje ved bruk av et eller flere utvalgskriterier for å rette innsamlingen mot spesifikke utenlandsetterretningsmål (f.eks. en bestemt kjent internasjonal terrorist eller terroristgruppe) eller spesifikke utenlandsetterretningsemner (f.eks. en fremmed makts eller dens agents spredning av masseødeleggelsesvåpen)».

([3]) Tilgjengelig på http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

De forente stater har utarbeidet prosesser for å sikre at signaletterretningsaktiviteter bare foretas for å fremme egnede formål knyttet til nasjonal sikkerhet. Hvert år fastsetter presidenten nasjonens høyeste prioriteringer for innsamling av utenlands-etterretning etter en omfattende og formell tverretatlig prosess. DNI har ansvar for å overføre disse etterretningsprioriteringene til National Intelligence Priorities Framework (NIPF). PPD-28 har styrket og forbedret den tverretatlige prosessen for å sikre at samtlige av etterretningssamfunnets etterretningsprioriteringer gjennomgås og godkjennes av beslutningstakere på høyt nivå. Intelligence Community Directive (ICD) 204 inneholder ytterligere veiledning om NIPF og ble oppdatert i januar 2015 for å omfatte kravene i PPD-28([1]). Selv om NIPF er gradert, angis det informasjon om spesifikke amerikanske utenlands-etterretningsprioriteringer årlig i DNIs ugraderte *Worldwide Threat Assessment*, som også er lett tilgjengelig på ODNIs nettsted.

Prioriteringene i NIPF er relativt generelle. De omfatter bl.a. bestemte utenlandske motstanderes utvikling av kjernefysisk kapasitet og kapasitet innen ballistiske missiler, virkningene av narkotikakartellrelatert korrupsjon og krenkelse av menneskerettighetene i bestemte land. Og de får ikke bare anvendelse på signaletterretning, men på alle etterretningsaktiviteter. Organisasjonen som har ansvar for å omgjøre prioriteringene i NIPF til konkret innsamling av signaletterretning, kalles National Signals Intelligence Committee (SIGCOM). SIGCOM arbeider under ledelse av direktøren for National Security Agency (NSA), som ved Executive Order 12333 er utpekt som «den funksjonelle lederen for signaletterretning» med ansvar for å føre tilsyn med og samordne signaletterretning i hele etterretningssamfunnet under tilsyn av både forsvarsministeren og DNI. SIGCOM har representanter fra alle enheter i etterretningssamfunnet, og etter hvert som De forente stater gjennomfører PPD-28 fullt ut, vil andre departementer og byråer med en politisk interesse i signaletterretning også bli representert fullt ut.

Alle amerikanske departementer og byråer som er forbrukere av utenlandsetterretning, inngir sine anmodninger om innsamling til SIGCOM. SIGCOM gjennomgår nevnte anmodninger, sikrer at de er i samsvar med NIPF og prioriterer dem ut fra kriterier som f.eks.:

— Kan signaletterretning gi nyttig informasjon i dette tilfellet, eller finnes det bedre eller mer kostnadseffektive kilder til informasjon som kan oppfylle behovet, f.eks. bilder eller informasjon fra åpne kilder?

— Hvor avgjørende er behovet for informasjon? Dersom det er en høy prioritering i NIPF, vil det som oftest være en høy signaletterretningsprioritering.

— Hvilken type signaletterretning kan benyttes?

— Er innsamlingen så målrettet som mulig? Bør det være tidsbegrensninger, geografiske begrensninger eller andre begrensninger?

Ved vurderingen av behovet for signaletterretning skal det også tas uttrykkelig hensyn til andre faktorer, nærmere bestemt:

— Er målet for innsamlingen eller innsamlingsmetoden spesielt sensitiv? Dersom dette er tilfellet, skal en overordnet beslutningstaker gjennomgå saken.

— Vil innsamlingen medføre en urimelig risiko for personvernet og de borgerlige frihetsrettighetene, uavhengig av statsborgerskap?

— Er ytterligere garantier med hensyn til spredning og lagring nødvendig for å ivareta personvernet eller nasjonale sikkerhetsinteresser?

Når prosessen er ferdig, bruker kompetent personell hos NSA prioriteringene som er godkjent av SIGCOM, for å søke etter og identifisere spesifikke utvalgskriterier, f.eks. telefonnumre eller e-postadresser, som forventes å føre til innsamling av utenlandsetterretning i samsvar med disse prioriteringene. Alle utvalgskriterier skal gjennomgås og godkjennes før de legges inn i NSAs innsamlingssystemer. Hvorvidt og når den faktiske innsamlingen finner sted, vil imidlertid til dels avhenge av andre

([1]) Tilgjengelig på http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

forhold, f.eks. tilgang til egnede innsamlingsressurser. Denne prosessen sikrer at målene for De forente staters innsamling av signaletterretning avspeiler gyldige og viktige utenlandsetterretningsbehov. Når innsamlingen foretas i henhold til FISA, må NSA og andre byråer selvfølgelig overholde de andre begrensningene som er godkjent av Foreign Intelligence Surveillance Court. Kort sagt kan verken NSA eller andre amerikanske etterretningsbyråer på egen hånd velge hva som skal samles inn.

Samlet sikrer denne prosessen at alle amerikanske etterretningsprioriteringer fastsettes av overordnede beslutningstakere som er best egnet til å identifisere De forente staters behov for utenlandsetterretning, og at disse beslutningstakerne tar høyde for ikke bare den potensielle verdien av etterretningsinnsamlingen, men også risikoene forbundet med slik innsamling, herunder risikoene for personvern, nasjonale økonomiske interesser og utenlandske relasjoner.

Selv om De forente stater ikke kan bekrefte eller avkrefte spesifikke etterretningsmetoder eller -aktiviteter, kan det opplyses om at når det gjelder opplysninger som overføres til De forente stater innenfor rammen av Privacy Shield-ordningen, får kravene i PPD-28 anvendelse på alle amerikanske signaletterretningsaktiviteter, uavhengig av typen av opplysninger som samles inn, eller kilden til disse. Begrensningene og garantiene som får anvendelse på innsamlingen av signaletterretning, får dessuten anvendelse på signaletterretning som samles inn i forbindelse med et godkjent formål, herunder formål knyttet til både utenlandske relasjoner og nasjonal sikkerhet.

Prosedyrene drøftet over viser at det er en klar vilje til å hindre vilkårlig innsamling av signaletterretningsinformasjon og til – på høyeste regjeringsnivå – å gjennomføre prinsippet om rimelighet. I PPD-28 og byråenes gjennomføringsprosedyrer avklares nye og eksisterende begrensninger for signaletterretning, og det redegjøres nærmere for formålet med De forente staters innsamling og bruk av signaletterretning. Disse bør gi sikkerhet for at signaletterretningsaktiviteter bare gjennomføres og fortsatt bare vil bli gjennomført for å fremme berettigede utenlandsetterretningsmål.

c. **Begrensninger for lagring og spredning**

I henhold til avsnitt 4 i PPD-28 skal hver enhet i etterretningssamfunnet ha uttrykkelige grenser for lagring og spredning av personopplysninger om ikke-amerikanske personer som er samlet inn gjennom signaletterretning, som kan sammenlignes med grensene som gjelder for amerikanske personer. Disse reglene er innarbeidet i prosedyrer for hvert enkelt etterretningsbyrå som ble utstedt i februar 2015, og som er offentlig tilgjengelige. Dersom personopplysninger skal kunne lagres eller spres som utenlandsetterretning, må de være knyttet til et godkjent etterretningsbehov, som fastsatt i NIPF-prosessen beskrevet over, med rimelighet kunne antas å være bevis på et lovbrudd eller oppfylle et av de andre kriteriene for oppbevaring av amerikanske personopplysninger beskrevet i avsnitt 2.3 i Executive Order 12333.

Opplysninger som ikke oppfyller noen av disse kriteriene, kan ikke oppbevares i mer enn fem år, med mindre DNI uttrykkelig beslutter at fortsatt oppbevaring er i De forente nasjoners nasjonale sikkerhets interesse. Enheter i etterretningssamfunnet skal derfor slette ikke-amerikanske personers personopplysninger som er samlet inn gjennom signaletterretning, fem år etter innsamlingen, med mindre det f.eks. er blitt fastslått at opplysningene er relevante for et godkjent behov for utenlandsetterretning, eller dersom DNI etter å ha vurdert synspunktene til ODNIs Civil Liberties Protection Officer og byråenes ansvarlige for personvern og borgerlige frihetsrettigheter, beslutter at fortsatt lagring er i den nasjonale sikkerhets interesse.

Det er dessuten et uttrykkelig krav i alle byråenes retningslinjer for gjennomføring av PPD-28 at opplysninger om en person ikke kan spres utelukkende med den begrunnelse at vedkommende ikke er amerikansk, og ODNI har utstedt et direktiv til alle enheter i etterretningssamfunnet([1]) om dette kravet. Etterretningssamfunnets personell skal særlig ta hensyn til personvern-interessene til ikke-amerikanske personer når de utarbeider utkast til og sprer etterretningsrapporter. Signaletterretning om en utenlandsk persons rutinemessige aktiviteter vil ikke bli ansett som utenlandsetterretning som kan spres eller oppbevares permanent alene på grunnlag av dette faktum, med mindre den på annen måte oppfyller et godkjent behov for utenlandsetterretning. Dette innebærer en viktig begrensning og er et svar på Europakommisjonens bekymringer over den brede definisjonen av utenlandsetterretning i Executive Order 12333.

([1]) Intelligence Community Directive (ICD) 203, tilgjengelig på http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Overholdelse og tilsyn**

Det amerikanske systemet for tilsyn med utenlandsetterretningsaktiviteter omfatter et strengt tilsyn på flere plan for å sikre overholdelse av gjeldende lover og prosedyrer, herunder om innsamling, lagring og spredning av ikke-amerikanske personers personopplysninger innsamlet gjennom signaletterretning i henhold til PPD-28. Dette omfatter følgende:

— Etterretningssamfunnet sysselsetter hundrevis av personer som arbeider med tilsynsoppgaver. Bare i NSA arbeider over 300 personer utelukkende med overholdelse, og andre etterretningsenheter har også tilsynskontorer. I tillegg fører justisdepartementet et omfattende tilsyn med etterretningsaktiviteter, og også i forsvarsdepartementet arbeides det med tilsyn.

— Hver enhet innen etterretningssamfunnet har sitt eget generalinspektørkontor (Office of the Inspector General) med ansvar for å føre tilsyn med blant annet utenlandsetterretningsaktiviteter. Generalinspektører («Inspectors Generals») har lovfestet uavhengighet og omfattende myndighet til å foreta undersøkelser, revisjoner og gjennomgåelser av programmer, herunder om bedrageri og misbruk eller overtredelse av loven, og kan anbefale korrigerende tiltak. Selv om generalinspektørenes anbefalinger ikke er bindende, offentliggjøres deres rapporter ofte, og de framlegges under alle omstendigheter for Kongressen. Dette omfatter oppfølgingsrapporter i de tilfellene der korrigerende tiltak anbefalt i tidligere rapporter ennå ikke er blitt gjennomført. Kongressen underrettes derfor om enhver manglende overholdelse og kan utøve press, herunder gjennom budsjettmidler, for å sikre at de korrigerende tiltakene gjennomføres. Det er offentliggjort en rekke rapporter fra generalinspektørene om etterretningsprogrammer([1]).

— ODNIs Civil Liberties and Privacy Office (CLPO) har ansvar for å sikre at etterretningssamfunnet opererer på en måte som fremmer den nasjonale sikkerheten og samtidig ivaretar de borgerlige frihetsrettighetene og personvernrettighetene([2]). Andre enheter i etterretningssamfunnet har egne personvernansvarlige.

— Privacy and Civil Liberties Oversight Board (PCLOB), et uavhengig organ opprettet ved lov, har ansvar for å analysere og gjennomgå terrorbekjempelsesprogrammer og -politikk, herunder bruken av signaletterretning, med henblikk på å sikre at personvernet og de borgerlige frihetsrettighetene ivaretas i tilstrekkelig grad. Det har utstedt en rekke offentlige rapporter om etterretningsaktiviteter.

— Som drøftet nærmere nedenfor har Foreign Intelligence Surveillance Court, en domstol bestående av uavhengige føderale dommere, ansvar for tilsyn og overholdelse når det gjelder innsamling av signaletterretning som gjennomføres i henhold til FISA.

— De forente staters kongress, særlig Representantenes hus' og Senatets etterretnings- og rettskomiteer, har et omfattende tilsynsansvar med hensyn til alle amerikanske utenlandsetterretningsaktiviteter, herunder amerikansk signaletterretning.

I tillegg til disse formelle tilsynsmekanismene har etterretningssamfunnet innført en rekke mekanismer for å sikre at det overholder begrensningene for innsamling beskrevet ovenfor. Dette gjelder for eksempel følgende:

— Kabinettet skal validere deres behov for signaletterretning hvert år.

— NSA kontrollerer signaletterretningsmålene i hele innsamlingsprosessen for å fastslå om de faktisk fører til innsamling av verdifull utenlandsetterretning i samsvar med prioriteringene, og vil stoppe innsamlingen i motsatt tilfelle. Ytterligere prosedyrer sikrer at utvalgskriteriene gjennomgås regelmessig.

([1]) Se f.eks. U.S. Department of Justice Inspector General Report «A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008» (september 2012), tilgjengelig på https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Se www.dni.gov/clpo.

— DNI har på grunnlag av en anbefaling fra et uavhengig granskingsutvalg nedsatt av president Obama opprettet en ny mekanisme for å overvåke innsamlingen og spredningen av signaletterretning som er spesielt sensitiv på grunn av målets art eller innsamlingsmetoden, for å sikre at dette er i samsvar med beslutningstakernes avgjørelser.

— ODNI foretar årlige gjennomgåelser av tildelingen av ressurser til etterretningssamfunnet ut fra prioriteringene i NIPF og etterretningsoppdraget som helhet. Denne gjennomgåelsen omfatter en vurdering av verdien av alle typer innsamling av etterretningsinformasjon, herunder signaletterretning, og man ser både bakover – i hvor stor grad har etterretningssamfunnet lykkes med å nå sine mål? – og framover – hva vil etterretningssamfunnet ha behov for i framtiden? Dette sikrer at signaletterretningsressursene anvendes på de viktigste nasjonale prioriteringene.

Slik det framgår av denne omfattende oversikten, beslutter etterretningssamfunnet ikke alene hvilke samtaler som skal avlyttes, det prøver ikke å samle inn alt, og det er underlagt kontroll. Etterretningssamfunnets aktiviteter fokuserer på prioriteringer fastsatt av beslutningstakere gjennom en prosess som hele regjeringen bidrar til, og som overvåkes både internt i NSA og av ODNI, justisdepartementet og forsvarsdepartementet.

PPD-28 inneholder også en rekke andre bestemmelser for å sikre vern av personopplysninger som samles inn gjennom signaletterretning, uavhengig av de berørte personenes statsborgerskap. I henhold til PPD-28 skal det f.eks. innføres datasikkerhets-, innsyns- og kvalitetsprosedyrer for å sikre vern av personopplysninger som samles inn gjennom signaletterretning, samt obligatorisk opplæring for å sikre at arbeidsstyrken forstår at det har et ansvar for å verne personopplysninger, uavhengig av statsborgerskap. I PPD er det også fastsatt andre tilsyns- og overholdelsesmekanismer. Dette innebærer at ansvarlige for tilsyn og overholdelse skal foreta regelmessige revisjoner og gjennomgåelser av metodene som brukes for å verne personopplysninger som inngår i signaletterretning. Gjennomgåelsene skal omfatte en undersøkelse av om byråene overholder prosedyrene for å verne slike opplysninger.

I PPD-28 er det også fastsatt at alvorlige tilfeller av manglende overholdelse knyttet til ikke-amerikanske personer skal behandles på høyeste regjeringsnivå. Ved alvorlige tilfeller av manglende overholdelse som omfatter personopplysninger samlet inn gjennom signaletterretning, skal de, i tillegg til eksisterende rapporteringskrav, rapporteres omgående til DNI. Dersom det er snakk om personopplysninger om en ikke-amerikansk person, skal DNI i samråd med utenriksministeren og lederen for den relevante enheten i etterretningssamfunnet beslutte om det bør treffes tiltak for å underrette den relevante utenlandske regjeringen i samsvar med vernet av kilder og metoder og av amerikansk personell. I henhold til PPD-28 har justisministeren dessuten utpekt en seniorkoordinator, statssekretær Catherine Novelli, som skal fungere som kontaktpunkt for utenlandske regjeringer som har spørsmål om De forente staters signaletterretningsaktiviteter. Dette engasjementet på høyt nivå illustrerer den innsatsen som den amerikanske regjering har gjort de siste årene for å skape tillit til de mange og overlappende tiltakene for å verne amerikanske og ikke-amerikanske personers personopplysninger.

e. **Sammendrag**

De forente staters prosesser for innsamling, lagring og spredning av utenlandsetterretning sikrer et omfattende vern av personopplysningene til alle personer, uavhengig av deres statsborgerskap. Disse prosessene sikrer særlig at vårt etterretningssamfunn fokuserer på sitt nasjonale sikkerhetsoppdrag i henhold til gjeldende lover, presidentordrer og presidentdirektiver, sikrer opplysningene mot uautorisert tilgang, bruk og utlevering og gjennomfører sine aktiviteter under tilsyn og kontroll på flere plan, herunder av Kongressens tilsynskomiteer. PPD-28 og prosedyrene som gjennomfører det, gjenspeiler vår innsats for å utvide visse prinsipper for minimering og andre viktige prinsipper for vern av opplysninger til å omfatte personopplysningene til alle personer, uavhengig av deres statsborgerskap. Personopplysninger samlet inn gjennom amerikansk signaletterretning omfattes av prinsippene og kravene i amerikansk rett og presidentdirektiver, herunder mekanismene for vern fastsatt i PPD-28. Disse prinsippene og kravene sikrer at alle personer behandles med verdighet og respekt, uavhengig av deres statsborgerskap eller bosted, og anerkjenner at alle personer har berettigede personverninteresser når det gjelder behandlingen av deres personopplysninger.

II. FOREIGN INTELLIGENCE SURVEILLANCE ACT — AVSNITT 702

Innsamling i henhold til avsnitt 702 i Foreign Intelligence Surveillance Act([1]) er ikke «massiv og vilkårlig», men er spesifikt rettet mot innsamling av utenlandsetterretning fra individuelt identifiserte berettigede mål, er tydelig hjemlet i lov og er gjenstand for både uavhengig rettslig tilsyn og omfattende gjennomgåelse og tilsyn innen den utøvende gren og Kongressen. Innsamling i henhold til avsnitt 702 anses som signaletterretning som er underlagt kravene i PPD-28([2]).

Innsamling i henhold til avsnitt 702 er en av de mest verdifulle etterretningskilder som beskytter både De forente stater og våre europeiske partnere. Det er offentliggjort omfattende informasjon om gjennomføring av og tilsyn med avsnitt 702. En rekke saksdokumenter, rettslige avgjørelser og tilsynsrapporter knyttet til programmet er blitt nedgradert og offentliggjort på ODNIs nettsted for offentliggjøring av dokumenter: www.icontherecord.tumblr.com. Avsnitt 702 er i tillegg blitt grundig analysert av PCLOB i en rapport som er tilgjengelig på https://www.pclob.gov/library/702-Report.pdf([3]).

Avsnitt 702 ble vedtatt som en del av FISA Amendments Act fra 2008([4]) etter en omfattende offentlig debatt i Kongressen. Det tillater innhenting av utenlandsetterretningsinformasjon gjennom målrettet overvåking av ikke-amerikanske personer som befinner seg utenfor De forente stater, med obligatorisk bistand fra amerikanske leverandører av elektroniske kommunikasjonstjenester. Avsnitt 702 bemyndiger den amerikanske justisministeren og DNI – to regjeringstjenestemenn utnevnt av presidenten og godkjent av Senatet – til å inngi årlige sertifiseringer til FISA-domstolen([5]). I disse sertifiseringene identifiseres særlige kategorier av utenlandsetterretning som skal samles inn, f.eks. etterretning knyttet til terrorbekjempelse eller masseødeleggelsesvåpen, som må falle inn under kategoriene av utenlandsetterretning som er fastsatt i FISA([6]). Som PCLOB har bemerket «tillater disse begrensningene *ikke* ubegrenset innsamling av informasjon om utlendinger»([7]).

Sertifiseringene skal også inneholde målrettings- og minimeringsprosedyrer som skal gjennomgås og godkjennes av FISA-domstolen([8]). Målrettingsprosedyrene er utformet for å sikre at innsamlingen bare skjer i henhold til de metodene som er godkjent ved lov, og i henhold til sertifiseringenes virkeområde. Minimeringsprosedyrene er utformet for å begrense innsamling, spredning og lagring av opplysninger om amerikanske personer, men inneholder også bestemmelser som sikrer et omfattende vern av opplysninger om ikke-amerikanske personer, som beskrevet nedenfor. Som beskrevet ovenfor har presidenten i PPD-28 pålagt etterretningssamfunnet å sørge for et ytterligere vern av personopplysninger om ikke-amerikanske personer, og nevnte vern får anvendelse på opplysninger som samles inn i henhold til avsnitt 702.

Når domstolen har godkjent målrettings- og minimeringsprosedyrene, kan innsamling i henhold til 702 ikke være massiv eller vilkårlig, men «utelukkende rettes mot spesifikke personer som det er truffet en individuell beslutning om», ifølge PCLOB([9]). Innsamlingen målrettes ved bruk av individuelle utvalgskriterier, f.eks. e-postadresser eller telefonnumre, som ifølge

([1]) 50 U.S.C. § 1881a.

([2]) De forente stater kan også innhente rettsavgjørelser i henhold til andre bestemmelser i FISA med henblikk på produksjon av opplysninger, herunder opplysninger som overføres innenfor rammen av Privacy Shield-ordningen. Se 50 U.S.C. § 1801 et seq. Titles I og III i FISA, som tillater henholdsvis elektronisk overvåking og fysiske søk, krever en rettsavgjørelse (bortsett fra i nødssituasjoner) og krever alltid at det skal være en rimelig grunn til å anta at målet er en fremmed makt eller en representant for en fremmed makt. Title IV i FISA tillater bruk av utstyr for registrering av oppringte numre fra et bestemt telefonnummer («pen register») og samtalesporingsutstyr («trap and trace»-utstyr), i henhold til en rettsavgjørelse (bortsett fra i nødssituasjoner) i forbindelse med godkjent etterforskning knyttet til utenlandsetterretning, kontraspionasje og terrorbekjempelse. I henhold til Title V i FISA kan FBI, i henhold til en rettsavgjørelse (bortsett fra i nødssituasjoner), få utlevert forretningsopplysninger som er relevante for godkjent etterforskning knyttet til utenlandsetterretning, kontraspionasje eller terrorbekjempelse. Som drøftet nedenfor forbyr USA FREEDOM Act spesifikt bruk av FISA-rettsavgjørelser om bruk av utstyr for registrering av oppringte numre fra et bestemt telefonnummer («pen register») og forretningsopplysninger til masseinnsamling, og krever at det brukes et «spesifikt utvalgskriterium» for å sikre at denne myndigheten brukes på en målrettet måte.

([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-rapporten»).

([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-rapporten, s. 99.

([8]) Se 50 U.S.C. § 1881a (d) og (e).

([9]) Se PCLOB-rapporten, s. 111.

amerikansk etterretningspersonells vurdering trolig vil bli brukt til å kommunisere utenlandsetterretningsinformasjon av den typen som omfattes av sertifiseringen inngitt til domstolen([1]). Grunnlaget for utvelgelse av målet skal dokumenteres, deretter gjennomgås dokumentasjonen for hvert utvalgskriterium av justisdepartementet([2]). Den amerikanske regjering har offentliggjort informasjon som viser at i 2014 ble rundt 90 000 privatpersoner overvåket i henhold til avsnitt 702, noe som utgjør en svært liten andel av de over 3 milliarder internettbrukerne over hele verden([3]).

Opplysninger som samles inn i henhold til avsnitt 702, omfattes av de domstolsgodkjente minimeringsprosedyrene som beskytter både ikke-amerikanske og amerikanske personer, og som er blitt offentliggjort([4]). Kommunikasjon som oppfanges i henhold til avsnitt 702, enten den gjelder amerikanske eller ikke-amerikanske personer, lagres f.eks. i databaser med streng tilgangskontroll. Kommunikasjonen kan bare gjennomgås av etterretningspersonell som har fått opplæring i de personvern-relaterte minimeringsprosedyrene, og som er blitt spesifikt godkjent for nevnte tilgang, slik at de kan utføre sine godkjente funksjoner([5]). Opplysningene kan bare brukes til identifisering av utenlandsetterretningsinformasjon eller som bevis på et lovbrudd([6]). I henhold til PPD-28 kan disse opplysningene bare spres dersom det foreligger et gyldig utenlandsetterretnings- eller rettshåndhevingsformål; utelukkende det faktum at en av partene i kommunikasjonen ikke er amerikansk, er ikke tilstrekkelig([7]). Og i minimeringsprosedyrene og PPD-28 er det også fastsatt grenser for hvor lenge opplysninger samlet inn i henhold til avsnitt 702 kan oppbevares([8]).

Tilsynet med avsnitt 702 er omfattende og utføres av alle de tre grenene av vårt statsapparat. I byråer som gjennomfører loven, utføres det internkontroll på flere plan, herunder av uavhengige generalinspektører, og teknologisk kontroll av tilgangen til opplysninger. Justisdepartementet og ODNI foretar en nøye gjennomgåelse og kontroll av anvendelsen av avsnitt 702 for å sikre at reglene overholdes. Byråene er også selv forpliktet til å rapportere om potensielle tilfeller av manglende overholdelse. Disse tilfellene undersøkes, og alle tilfeller av manglende overholdelse rapporteres til Foreign Intelligence Surveillance Court, President's Intelligence Oversight Board og Kongressen og rettes opp på egnet måte([9]). Hittil har det ikke vært noen tilfeller av forsettlige forsøk på å bryte loven eller å omgå lovfestede krav([10]).

FISA-domstolen spiller en viktig rolle når det gjelder gjennomføring av avsnitt 702. Den består av uavhengige føderale dommere som sitter i en sjuårsperiode ved FISA-domstolen, men som er dommere på livstid, i likhet med alle føderale dommere. Som angitt ovenfor må domstolen gjennomgå de årlige sertifiseringene og målrettings- og minimeringsprosedyrene for å sikre at de er i samsvar med loven. Som også angitt ovenfor skal offentlige myndigheter underrette domstolen umiddelbart om tilfeller av manglende overholdelse([11]). En rekke av domstolens uttalelser er også blitt nedgradert og offentliggjort og viser den ekstraordinære graden av rettslig kontroll og uavhengighet i domstolens gjennomgåelse av disse sakene.

Domstolens strenge prosesser er blitt beskrevet av dens tidligere rettsformann i et brev til Kongressen som er blitt offentliggjort([12]). Som følge av USA FREEDOM Act (beskrevet nedenfor) er domstolen nå uttrykkelig bemyndiget til å utnevne en ekstern advokat som uavhengig talsmann for personvern i saker som omfatter nye eller viktige juridiske spørsmål([13]). Denne graden av deltakelse av et lands uavhengige rettsapparat i utenlandsetterretningsaktiviteter rettet mot personer som verken er borgere i det aktuelle landet eller befinner seg i det, er uvanlig, om ikke uten presedens, og bidrar til å sikre at innsamling i henhold til avsnitt 702 skjer innenfor egnede rettslige grenser.

([1]) *Id.*

([2]) *Id.* s. 8, 50 U.S.C. § 1881a (l), se også NSAs Director of Civil Liberties and Privacy Report, «NSA's Implementation of Foreign Intelligence Surveillance Act Section 702» (heretter kalt «NSA-rapporten») s. 4, tilgjengelig på http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

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

([4]) Minimeringsprosedyrer er tilgjengelig på 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 på http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Se NSA-rapporten, s. 4.

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

([7]) Etterretningsbyråenes PPD-28-prosedyre er tilgjengelig på http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Se NSA Minimization Procedures, avsnitt 4 i PPD-28.

([9]) Se 50 U.S.C. § 1881 (l), se også PCLOB-rapporten på side 66–76.

([10]) Se Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, inngitt av den amerikanske justisministeren og direktøren for National Intelligence på s. 2–3, tilgjengelig på 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 Foreign Intelligence Surveillance Court Rules of Procedures, tilgjengelig på http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) 29. juli 2013, brev fra Reggie B. Walton til Patrick J. Leahy, tilgjengelig på http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Se avsnitt 401 i USA FREEDOM Act, P.L. 114–23.

Kongressen utøver tilsyn gjennom lovfestede rapporter til etterretnings- og rettskomiteene samt hyppige gjennomgåelser og høringer. Dette omfatter en halvårsrapport fra den amerikanske justisministeren som dokumenterer anvendelsen av avsnitt 702 og eventuelle tilfeller av manglende overholdelse([1]), en separat halvårsrapport fra justisministeren og DNI som dokumenterer overholdelsen av målrettings- og minimeringsprosedyrene, herunder overholdelsen av prosedyrene utarbeidet for å sikre at innsamlingen skjer i forbindelse med et gyldig utenlandsetterretningsformål([2]), og en årlig rapport fra ledere for enheter i etterretningssamfunnet som sertifiserer at innsamlingen i henhold til avsnitt 702 fortsatt genererer utenlands-etterretningsinformasjon([3]).

Kort sagt er innsamling i henhold til avsnitt 702 tillatt ved lov, er gjenstand for gjennomgåelser, rettslig overvåking og tilsyn på flere plan, og, som FISA-domstolen uttalte i en nylig nedgradert uttalelse, «utføres ikke på en vilkårlig eller massiv måte», men «ved hjelp av ... velavgrensede avgjørelser om målrettet overvåking av individuelle [kommunikasjons-]fasiliteter»([4]).

III. USA FREEDOM ACT

USA FREEDOM Act, som ble kunngjort i juni 2015, førte til en vesentlig endring innen amerikanske overvåkingsmyndigheter og andre nasjonale sikkerhetsmyndigheter, og ga økt offentlig åpenhet om bruken av disse myndighetene og om avgjørelser fra FISA-domstolen, som beskrevet nedenfor([5]). Loven sikrer at amerikanske etterretningstjenester og rettshåndhevingsorganer har den myndigheten de trenger for å beskytte nasjonen, og samtidig sikre et egnet personvern for den enkelte når denne myndigheten utøves. Den styrker personvernet og de borgerlige frihetsrettighetene og øker åpenheten.

Loven forbyr masseinnsamling av opplysninger, herunder om både amerikanske og ikke-amerikanske personer, i henhold til forskjellige bestemmelser i FISA eller ved bruk av nasjonale sikkerhetsbrev (NSL), en form for lovfestede administrative pålegg([6]). Dette forbudet omfatter spesifikt telefonmetadata om samtaler mellom personer i De forente stater og personer utenfor De forente stater, og vil også omfatte innsamling av Privacy Shield-opplysninger i henhold til disse myndighetene. I henhold til loven skal offentlige myndigheter basere alle anmodninger om opplysninger innenfor rammen av disse myndighetene på et «spesifikt utvalgskriterium» («specific selection term») – dvs. et søkekriterium som spesifikt identifiserer en person, konto, adresse eller personlig utstyr på en måte som begrenser omfanget av opplysningene det anmodes om, i den grad det kan la seg gjøre([7]). Dette innebærer en ytterligere garanti om at innsamling av opplysninger for etterretningsformål er nøye målrettet.

Loven har også i vesentlig grad endret prosedyrene ved FISA-domstolen ved både å gjøre dem mer åpne og å gi ytterligere garantier for at personvernet vil bli sikret. Som nevnt ovenfor tillater den at det opprettes et fast panel av sikkerhetsklarerte advokater med ekspertise innen personvern og borgerlige frihetsrettigheter, innsamling av etterretningsinformasjon, kommunikasjonsteknologi eller andre relevante områder, og de kan møte for domstolen som *amicus curiae* i saker som omfatter vesentlige eller nye fortolkninger av lovgivningen. Disse advokatene har myndighet til å framsette rettslige argumenter som utvider privatpersoners personvern og borgerlige frihetsrettigheter, og de vil ha tilgang til all informasjon, herunder gradert informasjon, som domstolen anser som nødvendig for at de skal kunne utføre sine oppgaver([8]).

Loven bygger også på den amerikanske regjerings nye og unike åpenhet rundt etterretningsaktiviteter som innebærer at det nå stilles krav til at DNI i samråd med den amerikanske justisministeren enten skal nedgradere eller offentliggjøre et ugradert sammendrag av alle avgjørelser, kjennelser eller uttalelser utstedt av FISA-domstolen eller Foreign Intelligence Surveillance Court of Review som inneholder en vesentlig forklaring eller fortolkning av lovbestemmelser.

([1]) Se 50 U.S.C. § 1881f.
([2]) Se *id*. § 1881a (l) (1).
([3]) Se *id*. § 1881a (l) (3). Noen av disse rapportene er graderte.
([4]) Uttalelse og avgjørelse, 26 (FISC 2014), tilgjengelig på 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 *id*. §§ 103, 201, 501. Nasjonale sikkerhetsbrev (NSL) har hjemmel i en rekke lover og gir FBI mulighet til å innhente opplysninger i kredittrapporter, finansielle dokumenter og elektroniske abonnent- og transaksjonsregistre fra visse typer selskaper, utelukkende med det som mål å verne mot internasjonal terrorisme og hemmelige etterretningsaktiviteter. Se 12 U.S.C. § 3414, 15 U.S.C. §§ 1681u–1681v, 18 U.S.C. § 2709. FBI bruker vanligvis nasjonale sikkerhetsbrev (NSL) til innsamling av kritiske innholdsløse opplysninger i de tidlige fasene av undersøkelser knyttet til terrorbekjempelse og kontraspionasje – f.eks. identiteten til en abonnent som kan ha kommunisert med agenter i en terroristgruppe, f.eks. IS. Mottakere av et nasjonalt sikkerhetsbrev (NSL) har rett til å bestride dette ved domstolene. Se 18 U.S.C. § 3511.
([7]) Se *id*.
([8]) Se *id*. § 401.

Loven sørger også for omfattende åpenhet om innsamling i henhold til FISA og om anmodninger om nasjonale sikkerhetsbrev (NSL). Den amerikanske regjering skal hvert år underrette Kongressen og allmennheten om antall FISA-kjennelser og -sertifiseringer som det er anmodet om, og som er oppnådd, om anslag over antall overvåkede og berørte amerikanske og ikke-amerikanske personer samt antall utnevnelser av *amici curiae*([1]). I henhold til loven skal regjeringen også offentliggjøre antall anmodninger om nasjonale sikkerhetsbrev (NSL) om både amerikanske og ikke-amerikanske personer([2]).

Med hensyn til åpenhet i virksomheter gir loven selskaper en rekke muligheter til å offentliggjøre det samlede antallet FISA-kjennelser og -direktiver eller nasjonale sikkerhetsbrev (NSL) som de mottar fra offentlige myndigheter, samt antall kundekontoer som er omfattet av disse kjennelsene([3]). En rekke selskaper har allerede offentliggjort dette, noe som har vist at det bare er blitt anmodet om opplysninger om et begrenset antall kunder.

Disse innsynsrapportene viser at amerikanske etterretningsanmodninger bare omfatter en svært liten del av alle opplysninger. Et stort selskaps nylige innsynsrapport viser f.eks. at de anmodningene som gjaldt nasjonale sikkerhetsformål (i henhold til FISA eller nasjonale sikkerhetsbrev (NSL)) som selskapet mottok, berørte færre enn 20 000 av dets kontoer på et tidspunkt da det hadde minst 400 millioner abonnenter. Med andre ord berørte samtlige anmodninger om opplysninger for nasjonale sikkerhetsformål færre enn 0,005 % av selskapets abonnenter. Selv om samtlige anmodninger hadde vedrørt «trygg havn»-opplysninger, noe som naturligvis ikke er tilfellet, er det åpenbart at anmodningene er målrettede og egnede med hensyn til omfang, og at det ikke er snakk om masseinnsamling eller vilkårlig innsamling.

Avslutningsvis understrekes det at selv om lovene som tillater bruk av nasjonale sikkerhetsbrev (NSL), allerede begrenset de situasjonene der en mottaker av et slikt brev kunne nektes å offentliggjøre det, er det fastsatt i loven at slike krav om hemmelighold skal gjennomgås regelmessig, og at mottakere av et nasjonalt sikkerhetsbrev (NSL) skal underrettes når de faktiske forholdene ikke lenger støtter et krav om hemmelighold, i tillegg til at loven inneholder kodifiserte framgangsmåter for mottakere som ønsker å bestride krav om hemmelighold([4]).

De viktige endringene innen de amerikanske etterretningsmyndighetene som ble innført med USA FREEDOM Act, er dermed et klart bevis på De forente staters omfattende innsats for å sette vern av personopplysninger, personvern, borgerlige frihetsrettigheter og åpenhet i sentrum for all amerikansk etterretningspraksis.

IV. ÅPENHET

I tillegg til åpenheten som er fastsatt i USA FREEDOM Act, gir det amerikanske etterretningssamfunnet allmennheten en stor mengde ytterligere informasjon og statuerer dermed et godt eksempel med hensyn til åpenhet i amerikanske etterretningsaktiviteter. Etterretningssamfunnet har offentliggjort en rekke av sine retningslinjer, prosedyrer, avgjørelser fra Foreign Intelligence Surveillance Court og annet nedgradert materiale, noe som gir en ekstraordinær høy grad av åpenhet. I tillegg offentliggjør etterretningssamfunnet betydelig mer statistikk over hvordan regjeringen bruker sin myndighet til å samle inn opplysninger for nasjonale sikkerhetsformål. Etterretningssamfunnet utstedte 22. april 2015 sin andre årlige rapport med statistikk over hvor ofte regjeringen anvender denne viktige myndigheten. ODNI har på sitt nettsted og på *IC On the Record* offentliggjort en rekke konkrete prinsipper for åpenhet([5]) og en gjennomføringsplan der prinsippene omgjøres til konkrete og målbare initiativer([6]). I oktober 2015 påla direktøren for National Intelligence de enkelte etterretningsbyråene å utpeke en ansvarlig for åpenhet i etterretningsaktiviteter på ledelsesnivå for å fremme åpenhet og stå i spissen for initiativer på dette området([7]). Denne ansvarlige vil samarbeide tett med de ansvarlige for personvern og borgerlige frihetsrettigheter i hvert etterretningsbyrå for å sikre at åpenhet, personvern og borgerlige frihetsrettigheter forblir topprioriteringer.

([1]) Se *id.* § 602.
([2]) Se *id.*
([3]) Se *id.* § 603.
([4]) Se *id.* §§ 502(f)–503.
([5]) Tilgjengelig på http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) Tilgjengelig på http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Se *id.*

Som et eksempel på denne innsatsen har NSAs Chief Privacy and Civil Liberties Officer frigitt flere ugraderte rapporter de siste årene, herunder rapporter om aktiviteter i henhold til avsnitt 702, Executive Order 12333 og USA FREEDOM Act([1]). I tillegg samarbeider etterretningssamfunnet tett med PCLOB, Kongressen og andre amerikanske aktører på området personvern for å fremme ytterligere åpenhet rundt amerikanske etterretningsaktiviteter, når det er mulig, og idet det tas hensyn til behovet for å verne sensitive etterretningskilder og -metoder. Samlet sett er amerikanske etterretningsaktiviteter preget av samme eller mer åpenhet enn mange andre nasjoners etterretningsaktiviteter verden over, og åpenheten er så stor som mulig med tanke på behovet for å verne sensitive kilder og metoder.

Oppsummering av den omfattende åpenheten rundt amerikanske etterretningsaktiviteter:

— Etterretningssamfunnet har frigitt og offentliggjort flere tusen sider på nettet med domstolsuttalelser og byråprosedyrer der det redegjøres for de særlige prosedyrene og kravene som gjelder for amerikanske etterretningsaktiviteter. Vi har også frigitt rapporter om etterretningsbyråenes overholdelse av gjeldende begrensninger.

— Overordnede tjenestemenn i etterretningssamfunnet uttaler seg regelmessig offentlig om de rollene deres organisasjoner har, og om de aktivitetene de utfører, herunder beskrivelser av hvilke overholdelsordninger og -garantier som gjelder for deres arbeid.

— Etterretningssamfunnet har frigitt en rekke andre dokumenter om etterretningsaktiviteter i henhold til Freedom of Information Act.

— Presidenten har utstedt PPD-28 som offisielt legger ytterligere begrensninger på våre etterretningsaktiviteter, og ODNI har utstedt to offentlige rapporter om gjennomføringen av disse begrensningene.

— Etterretningssamfunnet er nå pålagt ved lov å frigi viktige rettslige uttalelser utstedt av FISA-domstolen eller sammendrag av disse uttalelsene.

— Offentlige myndigheter skal hvert år rapportere om omfanget av sin bruk av visse nasjonale sikkerhetsmyndigheter, og selskaper har også rett til å gjøre dette.

— PCLOB har utstedt flere detaljerte offentlige rapporter om etterretningsaktiviteter og vil fortsette å gjøre dette.

— Etterretningssamfunnet framlegger omfattende gradert informasjon til Kongressens tilsynskomiteer.

— DNI har utstedt prinsipper for åpenhet som styrer etterretningssamfunnets aktiviteter.

Denne omfattende åpenheten vil bli opprettholdt i framtiden. All informasjon som offentliggjøres, vil naturligvis være tilgjengelig for både handelsdepartementet og Europakommisjonen. Handelsdepartementets og Europakommisjonens årlige gjennomgåelse av gjennomføringen av Privacy Shield-ordningen vil gi Europakommisjonen mulighet til å drøfte eventuelle spørsmål som har oppstått som følge av ny, frigitt informasjon, samt eventuelle andre spørsmål som gjelder Privacy Shield-ordningen og måten den fungerer på, og departementet kan om ønskelig invitere representanter fra andre byråer, herunder etterretningssamfunnet, til å delta i denne gjennomgåelsen. Dette kommer naturligvis i tillegg til mekanismen fastsatt i PPD-28 som gir EU-medlemsstatene mulighet til å ta opp overvåkingsrelaterte bekymringer med en utpekt tjenestemann i utenriksdepartementet.

V. KLAGEADGANG

Amerikansk rett inneholder en rekke klagemuligheter for privatpersoner som har vært gjenstand for ulovlig elektronisk overvåking i forbindelse med formål knyttet til nasjonal sikkerhet. I henhold til FISA er retten til søke erstatning ved amerikanske domstoler ikke begrenset til amerikanske personer. En person som kan dokumentere sin søksmålskompetanse, har

([1]) Tilgjengelig på 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.

adgang til rettsmidler som gjør det mulig å klage på ulovlig elektronisk overvåking i henhold til FISA. I henhold til FISA kan personer som har vært utsatt for ulovlig elektronisk overvåking, f.eks. saksøke amerikanske statstjenestemenn personlig for å oppnå økonomisk erstatning, herunder straffeerstatning og dekning av advokathonorarer. Se 50 U.S.C. § 1810. Privatpersoner som kan dokumentere sin søksmålskompetanse, kan også anlegge sivilt søksmål for å oppnå økonomisk erstatning, herunder til dekning av saksomkostninger, mot De forente stater når opplysninger om dem framkommet som følge av elektronisk overvåking i henhold til FISA er blitt ulovlig eller forsettlig brukt eller utlevert. Se 18 U.S.C. § 2712. Dersom regjeringen akter å bruke eller utlevere opplysninger som er innhentet ved eller utledet av elektronisk overvåking av en fornærmet person i henhold til FISA, mot den fornærmede personen i rettslige eller administrative prosedyrer i De forente stater, skal den på forhånd underrette domstolen og den fornærmede personen om sin hensikt, og den fornærmede personen kan deretter bestride lovligheten av overvåkingen og anmode om å få opplysningene fjernet. Se 50 U.S.C. § 1806. I FISA er det også fastsatt strafferettslige sanksjoner mot privatpersoner som med hensikt foretar ulovlig elektronisk overvåking i lovens navn, eller som med hensikt bruker eller utleverer informasjon innhentet ved ulovlig overvåking. Se 50 U.S.C. § 1809.

EU-borgere har andre muligheter til å anlegge sak mot amerikanske statstjenestemenn for ulovlig statlig bruk av eller tilgang til opplysninger, herunder statstjenestemenn som bryter loven i forbindelse med ulovlig tilgang til eller bruk av opplysninger til påståtte formål knyttet til nasjonal sikkerhet. Computer Fraud and Abuse Act forbyr bevisst uautorisert tilgang (eller tilgang ut over autorisert tilgang) for å innhente opplysninger fra en finansinstitusjon, den amerikanske regjerings databehandlingssystemer eller datamaskintilgang via internett samt trusler om å skade beskyttede datamaskiner med henblikk på utpressing eller bedrageri. Se 18 U.S.C. § 1030. Enhver person, uansett statsborgerskap, som lider skade eller tap som følge av en overtredelse av denne loven, kan saksøke lovovertrederen (herunder en statstjenestemann) for å oppnå skadeserstatning, forbud eller påbud eller en annen rimelig erstatning i henhold til avsnitt 1030 (g), uavhengig av om det har vært anlagt straffesak, forutsatt at atferden involverer minst en av flere av omstendighetene som er fastsatt i loven. Electronic Communications Privacy Act (ECPA) regulerer offentlige myndigheters tilgang til lagrede elektroniske kommunikasjons- og transaksjonsregistre samt abonnentopplysninger som innehas av tredjepartsleverandører av kommunikasjonstjenester. Se 18 U.S.C. §§ 2701–2712. I henhold til ECPA kan en fornærmet person saksøke statstjenestemenn for bevisst ulovlig tilgang til lagrede opplysninger. ECPA får anvendelse på alle personer uavhengig av deres statsborgerskap, og fornærmede personer kan få tilkjent skadeserstatning og få dekket advokathonorarer. Right to Financial Privacy Act (RFPA) begrenser den amerikanske regjerings tilgang til bankers og børsmegleres registre over privatkunder. Se 12 U.S.C. §§ 3401–3422. I henhold til RFPA kan en bank- eller børsmeglerkunde saksøke den amerikanske regjering med henblikk på å oppnå lovbestemt og faktisk erstatning samt straffeerstatning for urettmessig tilgang til kundens opplysninger, og dersom det konstateres at en slik urettmessig tilgang var forsettlig, innledes det automatisk en undersøkelse av om de relevante statsansatte skal ilegges disiplinære sanksjoner. Se 12 U.S.C. § 3417.

Avslutningsvis understrekes det at det i Freedom of Information Act (FOIA) er fastsatt at alle personer kan søke om innsyn i føderale byråers eksisterende registre om et hvilket som helst emne, med unntak av visse kategorier av informasjon. Se 5 U.S.C. § 552 (b). Disse omfatter begrensninger når det gjelder innsyn i gradert informasjon knyttet til nasjonal sikkerhet, personopplysninger om andre privatpersoner og informasjon som gjelder etterforskning i forbindelse med rettshåndheving, og kan sammenlignes med de begrensningene som andre nasjoner pålegger i sine egne lover om innsyn. Disse begrensningene gjelder både for amerikanske og ikke-amerikanske personer. Tvister om utlevering av registre som det anmodes om i henhold til FOIA, kan påklages administrativt og deretter ved føderale domstoler. Domstolen skal treffe en de novo-avgjørelse om hvorvidt registrene tilbakeholdes på lovlig vis, 5 U.S.C. § 552 (a) (4) (B), og kan tvinge myndighetene til å gi innsyn i registre. I noen tilfeller har domstolene omstøtt myndighetenes avgjørelser om at informasjon ikke skal utleveres fordi den er gradert([1]). Selv om det ikke gis skadeserstatning, kan domstolene tilkjenne et beløp til dekning av advokathonorar.

VI. KONKLUSJON

De forente stater anerkjenner at det i våre signaletterretnings- og andre etterretningsaktiviteter må tas hensyn til at alle personer bør behandles med verdighet og respekt, uavhengig av deres statsborgerskap eller bosted, og at alle personer har berettigede personverninteresser når det gjelder behandlingen av deres personopplysninger. De forente stater bruker bare signaletterretning for å fremme sine nasjonale sikkerhetsinteresser og utenrikspolitiske interesser og for å beskytte sine borgere og sine alliertes og partneres borgere mot skade. Kort sagt driver etterretningssamfunnet ikke vilkårlig overvåking av noen, herunder vanlige europeiske borgere. Innsamling av signaletterretning skjer bare når dette er behørig godkjent, og ved streng overholdelse av disse begrensningene samt først etter en vurdering av om det finnes tilgjengelige alternative kilder, herunder diplomatiske og

([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).

offentlige kilder, og på en måte som prioriterer egnede og mulige alternativer. I den grad det er praktisk mulig, finner signaletterretning dessuten bare sted gjennom innsamling rettet mot spesifikke utenlandske etterretningsmål eller -emner og ved bruk av diskriminanter.

De forente staters politikk på dette området ble bekreftet i PPD-28. De forente staters etterretningsbyråer har ikke rettslig myndighet, ressurser, teknisk kapasitet eller et ønske om å fange opp all kommunikasjon i verden innenfor denne rammen. Disse byråene leser ikke alle menneskers e-poster i De forente stater eller i verden. I samsvar med PPD-28 sikrer De forente stater et robust vern av ikke-amerikanske personers personopplysninger som samles inn gjennom signaletterretningsaktiviteter. I den grad det er praktisk mulig, og idet det tas hensyn til den nasjonale sikkerheten, omfatter dette retningslinjer og prosedyrer for å minimere lagring og spredning av personopplysninger om ikke-amerikanske personer som kan sammenlignes med det som gjelder for amerikanske personer. Som angitt ovenfor er den omfattende tilsynsordningen i henhold til avsnitt 702 i FISA uten motstykke. De omfattende endringene i De forente staters etterretningslovgivning som angis i USA FREEDOM Act og ODNIs initiativer for å fremme åpenhet i etterretningssamfunnet, øker i betydelig grad alle privatpersoners personvern og borgerlige frihetsrettigheter, uavhengig av deres statsborgerskap.

Vennlig hilsen

Robert S. Litt

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

Kjære Justin Antonipillai og Ted Dean

Jeg henvender meg til dere for å legge fram ytterligere informasjon om hvordan De forente stater foretar masseinnsamling av signaletterretning. Som forklart i fotnote 5 i Presidential Policy Directive 28 (PPD-28) viser «masseinnsamling» til innhenting av et forholdsvis stort volum av signaletterretningsinformasjon eller -data under omstendigheter der etterretningssamfunnet ikke kan bruke en identifikator knyttet til et bestemt mål (f.eks. målets e-postadresse eller telefonnummer) for å målrette innsamlingen. Dette betyr imidlertid ikke at denne formen for innsamling er «massiv» eller «vilkårlig». I PPD-28 kreves det dessuten at «signaletterretningsaktiviteter skal være så målrettede som mulig». Innenfor rammen av dette mandatet treffer etterretningssamfunnet tiltak for å øke sannsynligheten for at opplysningene som skal samles inn, selv når det ikke er mulig å bruke spesifikke identifikatorer for å målrette innsamlingen, inneholder utenlandsetterretning som oppfyller kravene fastsatt av amerikanske beslutningstakere i henhold til prosessen som det redegjøres for i mitt tidligere brev, og minimerer mengden av innsamlede opplysninger som ikke er relevante.

Etterretningssamfunnet kan f.eks. bli bedt om å samle inn signaletterretning om aktivitetene til en terroristgruppe som opererer i en region i en stat i Midtøsten, og som antas å planlegge angrep mot vesteuropeiske stater, men kjenner kanskje ikke navnene, telefonnumrene, e-postadressene til eller andre spesifikke identifikatorer på privatpersoner som er knyttet til denne terrorist-gruppen. Vi kan velge å foreta en målrettet overvåking av denne gruppen ved å samle inn kommunikasjon til og fra den aktuelle regionen for å gjennomgå og analysere den nærmere, slik at kommunikasjon knyttet til denne gruppen kan identifiseres. I denne forbindelse vil etterretningssamfunnet forsøke å avgrense innsamlingen så mye som mulig. Dette vil bli ansett som «masseinnsamling» fordi det ikke er mulig å bruke diskriminanter, men innsamlingen er verken «massiv» eller «vilkårlig», men isteden så nøyaktig målrettet som mulig.

Selv når det ikke er mulig å foreta målrettet innsamling ved bruk av spesifikke utvalgskriterier, samler De forente stater ikke inn all kommunikasjon fra alle kommunikasjonsfasiliteter overalt i verden, men bruker filtrer og andre tekniske verktøyer for å målrette innsamlingen til de fasilitetene der det er sannsynlighet for å samle inn kommunikasjon av verdi for utenlands-etterretningen. Dette sikrer at De forente staters signaletterretningsaktiviteter bare berører en brøkdel av den kommunikasjonen som skjer via internett.

Som bemerket i mitt tidligere brev, begrenser PPD-28 den bruken etterretningssamfunnet kan gjøre av masseinnsamlet signaletterretning til seks spesifikke formål, ettersom «masseinnsamling» innebærer en større risiko for at det samles inn ikke-relevant kommunikasjon. PPD-28 og byråenes politikk for gjennomføring av PPD-28 begrenser også lagring og spredning av personopplysninger som er samlet inn ved hjelp av signaletterretning, uavhengig av om opplysningene ble samlet inn via masseinnsamling eller målrettet innsamling, og uavhengig av privatpersonens statsborgerskap.

Etterretningssamfunnets «masseinnsamling» er derfor ikke «massiv» eller «vilkårlig», men innebærer bruk av metoder og verktøyer for å filtrere innsamlingen, slik at den rettes mot materiale som oppfyller beslutningstakernes uttrykte behov for utenlandsetterretning, samtidig som innsamlingen av ikke-relevante opplysninger minimeres, samt strenge regler for å verne

ikke-relevante opplysninger som eventuelt innhentes. Strategiene og prosedyrene beskrevet i dette brevet gjelder for all masseinnsamling av signaletterretning, herunder all masseinnsamling av kommunikasjon til og fra Europa, idet det verken bekreftes eller avkreftes at slik innsamling foregår.

Dere har også anmodet om mer informasjon om Privacy and Civil Liberties Oversight Board (PCLOB) samt om generalinspektører og den myndigheten det/de har. PCLOB er et uavhengig byrå innen den utøvende gren. Styret består av fem medlemmer fra de to største partiene som utnevnes av presidenten og godkjennes av Senatet([1]). Hvert av medlemmene i styret sitter i seks år. PCLOBs styremedlemmer og personale har den tilstrekkelige sikkerhetsklareringen som gjør at de kan utøve sine lovfestede plikter og ansvar([2]).

PCLOBs oppdrag er å sikre at den føderale regjerings innsats for å forebygge terrorisme står i et rimelig forhold til behovet for å ivareta personvernet og de borgerlige frihetsrettighetene. Styret har to grunnleggende ansvarsområder – tilsyn og rådgivning. PCLOB fastsetter sin egen dagsorden og bestemmer hvilke tilsyns- eller rådgivningsaktiviteter det ønsker å utføre.

I sin *tilsynsrolle* gjennomgår og analyserer PCLOB tiltak som den utøvende gren treffer for å verne nasjonen mot terrorisme, og sikrer dermed at behovet for slike tiltak står i et rimelig forhold til behovet for å ivareta personvernet og de borgerlige frihetsrettighetene([3]). I den siste gjennomgåelsen som PCLOB har foretatt på dette området, ble det fokusert på overvåkingsprogrammer gjennomført i henhold til avsnitt 702 i FISA([4]). PCLOB er i ferd med å foreta en gjennomgåelse av etterretningsaktiviteter gjennomført i henhold til Executive Order 12333([5]).

I sin *rådgivende* rolle sikrer PCLOB at det tas tilstrekkelig hensyn til frihetsaspekter i utarbeidingen og gjennomføringen av lover, regler og forskjellige typer politikk knyttet til innsatsen for å verne nasjonen mot terrorisme([6]).

For å kunne gjennomføre sitt oppdrag har styret lovfestet rett til å få tilgang til samtlige byråers relevante registre, rapporter, revisjoner, gjennomgåelser, dokumenter, papirer, anbefalinger og alt annet relevant materiale, herunder gradert informasjon i samsvar med loven([7]). I tillegg kan styret gjennomføre intervjuer og innhente uttalelser eller offentlige vitneutsagn fra enhver tjenestemann eller ansatt innen den utøvende gren([8]). Styret kan også skriftlig anmode den amerikanske justisministeren om å ta ut stevninger på vegne av styret for å tvinge parter utenfor den utøvende gren til å legge fram relevant informasjon([9]).

PCLOB er dessuten underlagt lovfestede krav til offentlig åpenhet. Dette omfatter å holde allmennheten informert om sine aktiviteter ved å avholde offentlige høringer samt ved å offentliggjøre sine rapporter, i den grad det er mulig på en måte som er forenlig med behovet for å sikre vern av graderte opplysninger([10]). PCLOB plikter i tillegg å rapportere når et byrå innen den utøvende gren nekter å følge PCLOBs råd.

Generalinspektører (Inspectors General) i etterretningssamfunnet foretar revisjoner, inspeksjoner og gjennomgåelser av programmene og aktivitetene i etterretningssamfunnet med henblikk på å identifisere og håndtere systemrelaterte risikoer, sårbare områder og mangler. Generalinspektører undersøker i tillegg klager på eller informasjon om påståtte overtredelser av lover, regler eller lovbestemmelser eller dårlig forvaltning, omfattende sløsing med midler, maktmisbruk eller en betydelig eller

([1]) 42 U.S.C. 2000ee (a), (h).
([2]) 42 U.S.C. 2000ee (k).
([3]) 42 U.S.C. 2000ee (d) (2).
([4]) Se https://www.pclob.gov/library.html#oversightreports.
([5]) Se 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, tilgjengelig på 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. 2000eee (f).

spesifikk fare for folkehelse eller offentlig sikkerhet i etterretningssamfunnets programmer og aktiviteter. Generalinspektørenes uavhengighet er av avgjørende betydning for å sikre objektivitet og integritet i deres rapporter, funn og anbefalinger. Noen av de viktigste faktorene for å sikre generalinspektørenes uavhengighet er bl.a. prosessen for utnevnelse og avsettelse, separat myndighet med hensyn til drift, budsjett og personell og kravene om dobbel rapportering til både lederne av byråene innen den utøvende gren og til Kongressen.

Kongressen har opprettet et uavhengig generalinspektørkontor i hvert byrå innen den utøvende gren, herunder i hver enhet i etterretningssamfunnet([1]). Som følge av vedtakelsen av Intelligence Authorization Act for Fiscal Year 2015 blir nesten alle generalinspektører med ansvar for tilsynet med en enhet i etterretningssamfunnet utnevnt av presidenten og godkjent av Senatet, herunder justisdepartementet, Central Intelligence Agency, National Security Agency og etterretningssamfunnet([2]). Disse generalinspektørene er dessuten fast ansatte tjenestemenn uten partitilknytning som bare kan avsettes av presidenten. Selv om presidenten ifølge den amerikanske grunnloven har myndighet til å avsette en generalinspektør, er denne myndigheten sjelden blitt utøvd, og det kreves at presidenten 30 dager før avsettelsen av en generalinspektør legger fram en skriftlig begrunnelse for Kongressen([3]). Denne prosessen for utnevnelse av generalinspektører sikrer at tjenestemenn innen den utøvende gren ikke utøver utilbørlig påvirkning på utvelgelsen, utnevnelsen eller avsettelsen av en generalinspektør.

Videre har generalinspektører omfattende lovbestemt myndighet til å foreta revisjoner, undersøkelser og gjennomgåelser av den utøvende grens programmer og aktiviteter. I tillegg til tilsynsundersøkelsene og -gjennomgåelsene som kreves i henhold til loven, har generalinspektørene svært frie hender når det gjelder å utøve tilsynsmyndighet for å gjennomgå programmer og aktiviteter etter eget valg([4]). I forbindelse med utøvelse av denne myndigheten sikrer loven at generalinspektørene har uavhengige ressurser for å utføre sine oppgaver, herunder myndighet til å ansette sitt eget personale og separat dokumentere sine budsjettanmodninger til Kongressen([5]). Loven sikrer at generalinspektører har tilgang til den informasjon de trenger for å kunne utføre sine oppgaver. Dette omfatter myndigheten til å få direkte tilgang til alle byråers registre samt informasjon om byråets programmer og aktiviteter uansett klassifisering, myndigheten til ved stevning å kreve framlegging av informasjon og dokumenter og myndigheten til å administrere edsavleggelse([6]). I begrensede tilfeller kan lederen for et byrå innen den utøvende gren forby en generalinspektørs aktivitet, f.eks. dersom en generalinspektørs revisjon eller undersøkelse i vesentlig grad vil skade De forente staters nasjonale sikkerhetsinteresser. Det er ekstremt sjelden at denne myndigheten utøves, og det krever at lederen for byrået underretter Kongressen innen 30 dager med en begrunnelse for dette([7]). Direktøren for National Intelligence har faktisk aldri utøvd denne myndigheten til å begrense generalinspektørenes aktiviteter.

Likeledes har generalinspektørene ansvar for at både lederne av byråene innen den utøvende gren og Kongressen holdes fullt ut og løpende orientert gjennom rapporter om bedrageri og andre alvorlige problemer samt misbruk og mangler knyttet til den utøvende grens programmer og aktiviteter([8]). Med dobbel rapportering styrkes generalinspektørenes uavhengighet, idet det gjør generalinspektørenes tilsynsprosesser mer åpne og gir lederne for byråene mulighet til å gjennomføre generalinspektørenes anbefalinger før Kongressen kan treffe lovgivningsmessige tiltak. Generalinspektørene er f.eks. ved lov forpliktet til å utarbeide halvårsrapporter der det redegjøres for slike problemer samt for korrigerende tiltak som hittil er truffet([9]). Byråer innen den utøvende gren tar generalinspektørenes konklusjoner og anbefalinger alvorlig, og generalinspektører kan ofte ta med byråenes

([1]) Avsnitt 2 og 4 i Inspector General Act fra 1978 med etterfølgende endringer (heretter kalt «IG Act»), avsnitt 103H (b) og (e) i National Security Act fra 1947, med etterfølgende endringer (heretter kalt «Nat'l Sec. Act»), avsnitt 17 (a) i Central Intelligence Act (heretter kalt «CIA Act»).

([2]) Se Pub. L. No 113-293, 128 Stat. 3990, (19. des. 2014). Det er bare generalinspektørene for Defense Intelligence Agency og National Geospatial-Intelligence Agency som ikke utnevnes av presidenten. Generalinspektøren for forsvarsdepartementet og generalinspektøren for etterretningssamfunnet har imidlertid delt myndighet over disse byråene.

([3]) Avsnitt 3 i IG Act fra 1978 med etterfølgende endringer, avsnitt 103H (c) i Nat'l Sec. Act og avsnitt 17 (b) i CIA Act.

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

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

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

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

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

([9]) Avsnitt 2 (3), 4 (a) og 5 i IG Act, avsnitt 103H (k) i Nat'l Sec. Act, avsnitt 17 (d) i CIA Act. Justisdepartementets generalinspektør gjør sine offentlig frigitte rapporter tilgjengelig på http://oig.justice.gov/reports/all.htm. Generalinspektøren for etterretningssamfunnet gjør sine halvårsrapporter offentlig tilgjengelig på https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

godkjenning og gjennomføring av generalinspektørenes anbefalinger i disse og andre rapporter som legges fram for Kongressen, og i noen tilfeller for allmennheten([1]). I tillegg til denne strukturen med dobbel rapportering har generalinspektørene også ansvar for at varslere innen den utøvende gren henvises til de riktige tilsynskomiteene i Kongressen for å avsløre påstått bedrageri, sløsing eller misbruk i den utøvende grens programmer og aktiviteter. Identiteten til dem som står fram, utleveres ikke til den utøvende gren, noe som beskytter varslerne mot mulige disiplinær- og sikkerhetsklareringstiltak som represalier for å ha underrettet generalinspektøren([2]). Ettersom varslere ofte er kilden i en generalinspektørs undersøkelse, gjør muligheten til å rapportere til Kongressen uten påvirkning fra den utøvende gren, generalinspektørens tilsyn mer effektivt. På grunn av denne uavhengigheten kan generalinspektørene fremme økonomi, effektivitet og ansvarlighet i byråene innen den utøvende gren med objektivitet og integritet.

Avslutningsvis har Kongressen også opprettet Council of Inspectors General on Integrity and Efficiency. Dette rådet utarbeider bl.a. standarder for generalinspektørenes revisjoner, undersøkelser og gjennomgåelser, fremmer opplæring og har myndighet til å foreta undersøkelser av påstått tjenesteforsømmelse blant generalinspektørene, med henblikk på å holde et våkent øye på generalinspektører som har fått ansvar for å overvåke alle andre([3]).

Jeg håper at denne informasjonen vil være til nytte.

Vennlig hilsen

Robert S. Litt

General Counsel

———

([1]) Avsnitt 2 (3), 4 (a) og 5 i IG Act, avsnitt 103H (k) i Nat'l Sec. Act, avsnitt 17 (d) i CIA Act. Justisdepartementets generalinspektør gjør sine offentlig frigitte rapporter tilgjengelig på http://oig.justice.gov/reports/all.htm. Likeledes gjør generalinspektøren for etterretningssamfunnet sine halvårsrapporter offentlig tilgjengelig på https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Avsnitt 7 i IG Act, avsnitt 103H (g) (3) i Nat'l Sec. Act, avsnitt 17 (e) (3) i CIA Act.

([3]) Avsnitt 11 i IG Act.

VEDLEGG VII

Brev fra Bruce Swartz, Deputy Assistant Attorney General and Counselor for International Affairs, De forente staters justisdepartement

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

Kjære Justin Antonipillai og Ted Dean

Dette brevet gir et kort overblikk over de viktigste undersøkelsesverktøyene som brukes til innhenting av forretningsopplysninger og andre opplysninger fra virksomheter i De forente stater for formål knyttet til strafferettslig håndheving eller allmennhetens interesse (sivilrettslige formål og reguleringsformål), herunder tilgangsbegrensningene som ledsager denne myndigheten([1]). Disse rettslige prosessene innebærer ikke forskjellsbehandling, ettersom de brukes til å innhente informasjon fra virksomheter i De forente stater, herunder fra selskaper som vil foreta egensertifisering innenfor rammen av Privacy Shield-avtalen mellom EU og De forente stater, uten hensyn til den registrertes statsborgerskap. Virksomheter som er gjenstand for en rettslig prosess i De forente stater, kan dessuten bestride dette ved domstolene som angitt nedenfor([2]).

Når det gjelder offentlige myndigheters beslagleggelse av opplysninger, er det verdt å merke seg det fjerde tillegget til De forente staters grunnlov der det fastslås at «folkets rett til sikkerhet for egen person, boliger, papirer og eiendeler mot urimelige ransakinger og beslagleggelser skal ikke krenkes, og det skal ikke avsies kjennelser uten at det foreligger en rimelig grunn understøttet av ed eller forsikring som særlig beskriver stedet som skal ransakes, personene som skal pågripes, eller tingene som skal beslaglegges.» Tillegg IV til De forente staters grunnlov. Som De forente staters høyesterett fastslo i *Berger v. State of New York*: «Det grunnleggende formålet med dette grunnlovstillegget, noe som er anerkjent i utallige av denne domstolens avgjørelser, er å sikre den enkeltes personvern og sikkerhet mot vilkårlige inngrep fra statstjenestemenn.» 388 U.S. 41, 53 (1967) (*Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). I henhold til fjerde grunnlovstillegg skal tjenestemenn i rettshåndhevende myndigheter generelt innhente en domstolskjennelse før en ransaking i forbindelse med innenlandsk strafferettslig etterforskning. Se *Katz v. United States*, 389 U.S. 347, 357 (1967). I de tilfellene der kravet om kjennelse ikke får anvendelse, er regjeringens aktiviteter underlagt en «rimelighetstest» i henhold til fjerde grunnlovstillegg. Grunnloven i seg selv sikrer derfor at den amerikanske regjering ikke har ubegrenset eller vilkårlig myndighet til å beslaglegge private opplysninger.

Strafferettshåndhevende myndigheter:

Føderale anklagere, som er tjenestemenn i det amerikanske justisdepartementet, og føderale etterforskningsagenter, herunder agenter i Federal Bureau of Investigation (FBI), et rettshåndhevende organ underlagt justisdepartementet, kan tvinge virksomheter i De forente stater til å legge fram dokumenter og andre registeropplysninger i forbindelse med strafferettslig

([1]) I denne oversikten redegjøres det ikke for de undersøkelsesverktøyene som rettshåndhevende myndigheter bruker for nasjonale sikkerhetsformål i forbindelse med etterforskning av terrorisme og annen etterforskning som gjelder nasjonal sikkerhet, herunder nasjonale sikkerhetsbrev (NSL) for visse registeropplysninger i kredittrapporter, finansielle dokumenter og elektroniske abonnent- og transaksjonsregistre, se 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, og for elektronisk overvåking, ransakingsordrer, forretningsopplysninger og annen innsamling av kommunikasjon i henhold til Foreign Intelligence Surveillance Act, se 50 U.S.C. § 1801 et seq.

([2]) I dette dokumentet redegjøres det for føderale rettshåndhevende myndigheter og reguleringsmyndigheter. Overtredelser av delstatslovene etterforskes av delstatene og behandles ved delstatsdomstolene. De rettshåndhevende myndighetene på delstatsplan bruker kjennelser og stevninger utstedt i henhold til delstatslovgivningen på stort sett samme måte som beskrevet her, men med den forskjellen at delstatenes rettslige prosesser kan omfattes av et vern fastsatt i delstatsgrunnloven som kan være strengere enn det som er fastsatt i den amerikanske grunnloven. Det vernet som sikres ved delstatslovgivningen må være minst det samme som det som sikres ved den amerikanske grunnloven, herunder, men ikke begrenset til, det fjerde grunnlovstillegget.

etterforskning gjennom flere forskjellige former for obligatoriske rettslige prosesser, herunder stevninger fra en storjury («grand jury subpoenas»), administrative pålegg («administrative subpoenas») og ransakingsordrer, og kan innhente annen kommunikasjon takket være føderale myndigheter med ansvar for avlytting i straffesaker og bruk av utstyr for registrering av oppringte numre fra et bestemt telefonnummer («pen register»).

Stevninger utstedt av en storjury («grand jury subpoena») eller i en rettssak («trial subpoenas»): Strafferettslige stevninger brukes til å støtte målrettet etterforskning i forbindelse med rettshåndheving. En stevning utstedt av en storjury er en offisiell anmodning fra en storjury (som regel på anmodning fra en føderal anklager) om å bistå i storjuryens etterforskning ved mistanke om overtredelse av straffeloven. Storjuryer er domstolens etterforskningsgren og oppnevnes av en dommer eller en fredsdommer. En stevning kan pålegge noen å vitne i en rettssak eller legge fram eller gjøre tilgjengelig forretningsopplysninger, elektronisk lagrede opplysninger eller andre håndgripelige elementer. Opplysningene må være relevante for etterforskningen, og pålegg kan ikke være urimelige, dvs. overdrevne, undertrykkende eller tyngende. En mottaker kan bestride en stevning med henvisning til disse grunnene. Se Fed. R. Crim. P. 17. I sjeldne situasjoner kan stevninger i rettsaker med pålegg om framlegging av dokumenter anvendes etter at storjuryen har reist tiltale.

Myndighet til å utstede administrative pålegg («administrative subpoenas)»: Det kan utstedes administrative pålegg i forbindelse med straffe- og sivilrettslige etterforskning. I forbindelse med strafferettslig håndheving tillater en rekke føderale lover at det utstedes administrative pålegg om å legge fram eller gjøre tilgjengelig forretningsopplysninger, elektronisk lagret informasjon eller andre håndgripelige elementer i etterforskning som omfatter misbruk av helsetjenesteytelser, overgrep mot barn, beskyttelse av etterretningstjenester, saker som gjelder kontrollerte stoffer, og i forbindelse med generalinspektørers undersøkelser av offentlige organer. Dersom offentlige myndigheter anmoder om å få håndhevet et administrativt pålegg ved en domstol, kan mottakeren av det administrative pålegget i likhet med mottakeren av en stevning utstedt av en storjury gjøre gjeldende at pålegget er urimelig fordi det er undertrykkende eller tyngende.

Rettsavgjørelser om utstyr for registrering av oppringte numre fra et bestemt telefonnummer («pen register») og samtalesporingsutstyr («trap and trace»): I henhold til de strafferettslige bestemmelsene som gjelder bruk av ovennevnte utstyr, kan rettshåndhevende myndigheter oppnå en rettsavgjørelse for å innhente innholdsløse opplysninger i sanntid om telefonoppringninger, ruting, adresser og signaler knyttet til et telefonnummer eller en e-postadresse etter å ha framlagt dokumentasjon på at de aktuelle opplysningene er relevante for en pågående strafferettslig etterforskning. Se 18 U.S.C. §§ 3121–3127. Bruk eller installasjon av slikt utstyr uten lovhjemmel er et føderalt lovbrudd.

Electronic Communications Privacy Act (ECPA): En rekke andre regler regulerer offentlige myndigheters tilgang til abonnentopplysninger, trafikkdata og lagret innhold i kommunikasjon som innehas av teleselskaper og andre tredjepartsleverandører, i henhold til Title II i ECPA, også kalt Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712. I SCA er det fastsatt en rekke lovbestemte personvernrettigheter som begrenser rettshåndhevende myndigheters tilgang til opplysninger ut over det som kreves i forfatningsretten, fra internettleverandørers kunder og abonnenter. I henhold til SCA økes personvernnivået ut fra hvor inngripende innsamlingen er. Strafferettshåndhevende myndigheter kan bare få utlevert abonnentopplysninger, IP-adresser og tilhørende tidsstempler samt faktureringsopplysninger på grunnlag av et pålegg. For de fleste andre lagrede, innholdsløse opplysninger, f.eks. e-postoverskrifter uten emnefeltet, må rettshåndhevende myndigheter legge fram spesifikke fakta for en dommer som viser at opplysningene det anmodes om, er relevante og av betydning for en pågående strafferettslig etterforskning. For å få utlevert lagret innhold i elektronisk kommunikasjon må strafferettshåndhevende myndigheter som regel få utstedt en fullmakt fra en dommer som bygger på at det er rimelig grunn til å tro at den aktuelle kontoen inneholder bevis på lovbrudd. I henhold til SCA kan det også ilegges erstatningsansvar og strafferettslige sanksjoner.

Rettsavgjørelser om overvåking i henhold til den føderale loven om avlytting: Rettshåndhevende myndigheter kan dessuten fange opp trådbasert, muntlig eller elektronisk kommunikasjon i sanntid i forbindelse med strafferettslige etterforskningsformål i henhold til den føderale loven om avlytting. Se 18 U.S.C. §§ 2510–2522. En slik tillatelse gis bare på grunnlag av en rettsavgjørelse der en dommer bl.a. finner at det er rimelig grunn til å tro at avlyttingen eller den elektroniske oppfangingen vil

framskaffe bevis på et føderalt lovbrudd, eller opplysninger om hvor en person som er på flukt for å unngå rettsforfølging, befinner seg. I henhold til loven kan det ilegges erstatningsansvar og strafferettslige sanksjoner for overtredelse av avlyttingsbestemmelsene.

Ransakingsordre – regel 41: Rettshåndhevende myndigheter kan foreta fysiske ransakinger av lokaler i De forente stater dersom de har fått tillatelse til dette fra en dommer. Rettshåndhevende myndigheter skal dokumentere overfor dommeren at det er «rimelig grunn» til å tro at det er blitt eller snart vil bli begått et lovbrudd, og at det er sannsynlig at elementer knyttet til lovbruddet vil bli funnet på stedet angitt i kjennelsen. En slik myndighet brukes ofte når det er nødvendig at politiet foretar en fysisk ransaking av et lokale fordi det er fare for bevisforspillelse dersom det utstedes et pålegg eller en annet beslutning om framlegging av dokumentasjon. Se tillegg IV til den amerikanske grunnloven (drøftet nærmere ovenfor), Fed. R. Crim. P. 41. Vedkommende som er mottaker av ransakingskjennelsen, kan treffe tiltak for å få kjent kjennelsen ugyldig med den begrunnelse at den er overdreven, sjikanerende eller på annen måte urettmessig avsagt, og fornærmede parter med søksmålskompetanse kan anmode om å få avvist alle bevis innhentet ved en ulovlig ransaking. Se *Mapp v. Ohio*, 367 U.S. 643 (1961).

Det amerikanske justisdepartementets retningslinjer og politikk: I tillegg til disse konstitusjonelle, lov- og regelbaserte begrensningene for offentlige myndigheters tilgang til opplysninger, har den amerikanske justisministeren utstedt retningslinjer som ytterligere begrenser rettshåndhevende myndigheters tilgang til opplysninger, og som også inneholder bestemmelser om personvern og vern av borgerlige frihetsrettigheter. I den amerikanske justisministerens retningslinjer, Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (september 2008) (heretter kalt AG FBI Guidelines), som er tilgjengelig på http://www.justice.gov/archive/opa/docs/guidelines.pdf, er det f.eks. fastsatt begrensninger for bruk av etterforskningsmetoder for å søke etter informasjon knyttet til etterforskning som involverer føderale lovbrudd. I henhold til disse retningslinjene skal FBI bruke minst mulig inngripende etterforskningsmetoder, idet det tas hensyn til hvilken innvirkning de har på personvernet og de borgerlige frihetsrettighetene samt den potensielle skaden på omdømmet. Det fastslås videre at «det er en selvfølge at FBI skal utføre sin etterforskning og andre aktiviteter på en lovlig og rimelig måte som respekterer frihet og personvern, og der man unngår unødvendige inngripen i lovlydige menneskers liv.» Se AG FBI Guidelines, s. 5. FBI har gjennomført disse retningslinjene gjennom FBI Domestic Investigations and Operations Guide (DIOG) som er tilgjengelig på https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), en omfattende håndbok som omfatter detaljerte grenser for bruk av undersøkelsesverktøyer og retningslinjer for å sikre at de borgerlige frihetsrettighetene og personvernet ikke krenkes i undersøkelsene. Det er fastsatt ytterligere regler og retningslinjer som begrenser de føderale anklagernes etterforskningsaktiviteter, i **United States Attorneys' Manual** (USAM), som også er tilgjengelig på http://www.justice.gov/usam/united-states-attorneys-manual.

Sivile myndigheter og reguleringsmyndigheter (allmennhetens interesse):

Det er også betydelige begrensninger for sivile myndigheters og reguleringsmyndigheters (*dvs*. «allmennhetens interesse») tilgang til opplysninger som innehas av virksomheter i De forente stater. Myndigheter med sivilrettslig ansvar og reguleringsansvar kan utstede pålegg til virksomheter om utlevering av forretningsopplysninger, elektronisk lagrede opplysninger eller andre håndgripelige elementer. Disse myndighetenes administrative eller sivilrettslige myndighet til å utstede pålegg er begrenset, ikke bare på grunn av egne regler, men også på grunn av uavhengig domstolsprøving av pålegg før en potensiell rettshåndheving. Se f.eks. Fed. R. Civ. P. 45. Myndighetene kan bare be om tilgang til opplysninger som er relevante for saker som omfattes av deres reguleringsmyndighet. En mottaker av et administrativt pålegg kan dessuten bestride håndhevingen av nevnte pålegg ved en domstol ved å legge fram bevis på at myndigheten ikke har opptrådt i samsvar med de grunnleggende standardene for rimelighet, som drøftet tidligere.

Virksomheter kan bestride anmodninger om utlevering av opplysninger fra forvaltningsmyndigheter med hjemmel i annet rettslig grunnlag, avhengig av sektoren og den typen opplysninger de innehar. Finansinstitusjoner kan f.eks. bestride administrative pålegg om utlevering av visse typer opplysninger med den begrunnelse at de er i strid med Bank Secrecy Act og bestemmelsene som gjennomfører denne loven. Se 31 U.S.C. § 5318, 31 C.F.R. del X. Andre virksomheter kan bruke Fair Credit Reporting Act, se 15 U.S.C. § 1681b, eller en rekke andre sektorspesifikke lover. Ved misbruk av et organs myndighet til å utstede pålegg kan organet eller tjenestemennene personlig trekkes til ansvar. Se f.eks. Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422. Domstoler i De forente stater utgjør således et vern mot urettmessige lovfestede anmodninger og fører uavhengig tilsyn med føderale byråers virksomhet.

Forvaltningsmyndighetenes lovfestede myndighet til å kunne fysisk beslaglegge registre fra en virksomhet i De forente stater i forbindelse med en administrativ ransaking, må oppfylle kravene i det fjerde grunnlovstillegget. Se *v. City of Seattle*, 387 U.S. 541 (1967).

Konklusjon

Alle rettshåndhevings- og reguleringsaktiviteter i De forente stater skal være i samsvar med gjeldende rett, herunder den amerikanske grunnloven, lover, regler og bestemmelser. Disse aktivitetene skal dessuten være i samsvar med gjeldende retningslinjer, herunder den amerikanske justisministerens generelle retningslinjer for håndheving av føderal rett. Den rettslige rammen beskrevet ovenfor begrenser de amerikanske rettshåndhevings- og reguleringsorganenes muligheter til å innhente opplysninger fra virksomheter i De forente stater – enten opplysningene gjelder amerikanske eller utenlandske borgere – og gir også mulighet for domstolsprøving av alle anmodninger om opplysninger fra offentlige myndigheter i henhold til denne myndigheten.

Vennlig hilsen

Bruce C. Swartz

Deputy Assistant Attorney General and Counselor for International Affairs