16/DA
WP 238

Udtalelse 01/2016 om udkast til afgørelse af tilstrækkeligheden af EU's og USA's værn om privatlivets fred

Vedtaget den 13. april 2016

RESUMÉ

Den 29. februar 2016 offentliggjorde Europa-Kommissionen en meddelelse, et udkast til en tilstrækkelighedsafgørelse og de vedlagte tekster, der udgør en ny ramme for transatlantiske udvekslinger af persondata til kommercielle formål: EU's og USA's værn om privatlivets fred (i det følgende benævnt: værnet om privatlivets fred), som har til hensigt at erstatte USA's tidligere Safe Harbour-principper, som blev gjort ugyldig af Den Europæiske Unions Domstol (i det følgende benævnt: EU-Domstolen) den 6. oktober 2015 i Schrems-sagen.

I henhold til artikel 30, stk. 1, litra c), i direktiv 95/46/EF vurderede artikel 29-arbejdsgruppen (i det følgende benævnt: WP29) disse dokumenter for at komme med sin udtalelse om udkastet til en tilstrækkelighedsafgørelse. WP29 vurderede både de kommercielle aspekter og de mulige undtagelsesbestemmelser for principperne for værnet om privatlivets fred til formål for national sikkerhed, retshåndhævelse og offentlige interesser.

WP29 tog højde for den gældende retslige ramme for databeskyttelse i EU som fremsat i direktiv 95/46/EF samt de grundlæggende rettigheder for beskyttelse af privatliv og data som fastlagt i artikel 8 i den europæiske menneskerettighedskonvention og artikel 7 og 8 i EU's charter om grundlæggende rettigheder. Den tog også højde for retten til et effektivt retsmiddel og til en retfærdig rettergang som fastlagt i artikel 47 i charteret samt retslæren i forbindelse med forskellige grundlæggende rettigheder.

Analysen giver endvidere udtryk for EU-Domstolens domspræmisser i Schrems-sagen vedrørende Kommissionens anerkendelsesmargin for en tilstrækkelighedsvurdering. Tjek og kontroller af tilstrækkelighedskravene skal strengt udføres, idet der tages højde for de grundlæggende rettigheder i forbindelse med privatlivets fred og databeskyttelse samt antallet af fysiske personer, der potentielt bliver påvirket af videregivelser.

Værnet om privatlivets fred skal ses i den aktuelle internationale kontekst, såsom fremkomsten af store data og de stigende sikkerhedsbehov. Anvendelsesområdet for og omfanget af indsamling og brug af personoplysninger er steget dramatisk, siden den oprindelige Safe Harbour-afgørelse blev truffet i 2000. Europæiske databeskyttelsesmyndigheder hævder vigtigheden af de principper, de forsvarer.

WP29 bifalder allerførst de væsentlige forbedringer, som værnet om privatlivets fred bringer, sammenlignet med Safe Harbour-afgørelsen. Den anfører, at forhandlerne har taget sig af mange af de utilstrækkeligheder ved Safe Harbour, som den havde påpeget i sit brev dateret 10. april 2014 til næstformand Viviane Reding.

Det faktum, at de principper og garantier, der gives af værnet om privatlivets fred, er fremsat i både tilstrækkelighedsafgørelsen og i dens bilag, gør informationen både vanskelig at finde og til tider selvmodsigende. Dette bidrager til en samlet mangel på klarhed i forbindelse med den nye ramme samt gør tilgængeligheden for registrerede, organisationer og databeskyttelsesmyndigheder vanskeligere. Ligeledes mangler det anvendte sprog klarhed.

Derfor opfordrer WP29 Kommissionen til at gøre dette klart og forståeligt for begge sider af Atlanterhavet.

Med hensyn til gældende lov fremhæver WP29, at hvis tilstrækkelighedsafgørelsen vedrørende værnet om privatlivets fred indføres på grundlag af direktiv 95/46/EF, skal den være i overensstemmelse med den retslige ramme for databeskyttelse i EU, både hvad angår anvendelsesområde og terminologi. WP29 mener, at en evaluering skal foretages kort efter ikrafttrædelsen af den generelle databeskyttelsesforordning for at sikre, at det højere niveau af databeskyttelse, som er indeholdt i forordningen, overholdes i tilstrækkelighedsafgørelsen og dens bilag.

Vedrørende de kommercielle aspekter ved værnet om privatlivets fred

WP29's primære formål er at sikre, at det praktisk talt tilsvarende beskyttelsesniveau, som tilvejebringes til fysiske personer, opretholdes, når persondata behandles afhængigt af bestemmelserne i værnet om privatlivets fred. Selv om WP29 ikke forventer, at værnet om privatlivets fred blot er en omfattende kopi af den retslige ramme i EU, anser den, at det bør indeholde de grundlæggende princippers hovedindhold og som følge deraf sikre et "praktisk talt tilsvarende" beskyttelsesniveau.

Til trods for forbedringerne, som tilbydes af værnet om privatlivets fred, anser WP29, at nogle nøgleprincipper vedrørende databeskyttelse som fremsat i europæisk lov ikke er afspejlet i udkastet til tilstrækkelighedsafgørelsen og bilagene eller ikke er blevet tilstrækkeligt erstattet af alternative begreber.

For eksempel er dataopbevaringsprincippet ikke udtrykkeligt nævnt og kan ikke fortolkes klart ud fra den nuværende formulering af dataintegritet og princippet om formålsbegrænsning. Der er endvidere ikke nogen formulering for den beskyttelse, der skal ydes mod automatiserede, individuelle beslutninger, udelukkende baseret på edb-behandling. Anvendelsen af princippet om formålsbegrænsning i forbindelse med databehandling er også uklar. For at bringe mere klarhed til anvendelsen af flere vigtige begreber giver WP29 udtryk for, at klare definitioner bør aftales mellem EU og USA samt være en del af en ordliste, som skal inkluderes i de ofte stillede spørgsmål vedrørende værnet om privatlivets fred.

Da værnet om privatlivets fred også skal bruges til at videregive data uden for USA, kræver WP29, at videregivelse fra en entitet omfattet af værnet om privatlivets fred til tredjelandsmodtagere skal yde samme beskyttelsesniveau for alle værnets aspekter (inklusive national sikkerhed) og ikke skal medføre lavere eller omgåede databeskyttelsesprincipper i EU. Hvis en videregivelse til et tredjeland forudses under værnet om privatlivets fred, skal alle organisationer under værnet om privatlivets fred være forpligtet til at vurdere alle obligatoriske krav for tredjelandets nationale lovgivning, der er gældende for dataimportøren, forud for videregivelsen. Generelt set konkluderer WP29, at rammerne for videregivelse af persondata fra EU er utilstrækkelige, særligt hvad angår deres anvendelsesområde, begrænsningen af deres formål og de garantier, der gælder for videregivelser til agenter.

Selv om WP29 anfører, at yderligere regresser er gjort tilgængelige for udøvelse af fysiske personer, er den bekymret over, at den nye afhjælpningsmekanisme i praksis kan vise sig at være for kompleks, vanskelig at bruge for fysiske personer i EU og derfor virkningsløs. Der er derfor behov for yderligere afklaring af de forskellige regresprocedurer; især kan databeskyttelsesmyndigheder i EU, hvor de er beredvillige, betragtes som et naturligt kontaktpunkt for fysiske personer i EU i de forskellige procedurer, hvor de har muligheden for at handle på deres vegne.

Undtagelsesbestemmelser til formål for national sikkerhed

Hvad angår offentlige myndigheders aktindsigt, både i EU og i tredjelande, minder WP29 om sin analyse af de relevante grundlæggende rettigheder, der er indeholdt i arbejdsdokumentet om basis for indgreb i de grundlæggende rettigheder for privatlivets fred og databeskyttelse gennem overvågningsforanstaltninger under videregivelse af persondata (europæiske essentielle garantier) (WP237).

Et stort skridt fremad fra Safe Harbour-afgørelsen er, at udkastet til tilstrækkelighedsafgørelsen nu i stor udstrækning omfatter den mulige aktindsigt behandlet under værnet om privatlivets fred til formål for national sikkerhed og retshåndhævelse. WP29 anerkender dette betydningsfulde skridt samt den øgede gennemsigtighed, som den amerikanske regering tilbyder i forbindelse med lovgivningen, der gælder for indsamling af efterretningsdata (Bilag VI).

WP29 anfører imidlertid, at det amerikanske Office of the Director of National Intelligence (ODNI) ikke ekskluderer stor og vilkårlig indsamling af persondata, der stammer fra EU. WP29 minder om sin mangeårige holdning om, at stor og vilkårlig overvågning af fysiske personer aldrig kan anses som forholdsmæssig og strengt nødvendigt i et demokratisk samfund, som det er påkrævet under beskyttelsen, som ydes af de gældende, grundlæggende rettigheder. Endvidere er et omfattende tilsyn med alle overvågningsprogrammer afgørende. WP29 bemærker, at der er en tendens til at indsamle endnu flere data på en stor og vilkårlig skala set i lyset af kampen mod terrorisme. Set i lyset af de bekymringer, dette medfører for beskyttelsen af de grundlæggende rettigheder for privatlivets fred og databeskyttelse, henviser WP29 til EU-Domstolens forestående kendelser i sager vedrørende stor og vilkårlig dataindsamling.

Hvad angår afhjælpning bifalder WP29 stiftelsen af en Ombudsperson som en ny afhjælpningsmekanisme. Dette kan udgøre en betydningsfuld forbedring for fysiske personer i EU's rettigheder, hvad angår amerikanske efterretningsaktiviteter. WP29 er imidlertid bekymret over, at denne nye institution ikke er tilstrækkeligt uafhængig og ikke er udstyret med tilstrækkelig bemyndigelse til effektivt at udøve sin pligt og ikke garanterer et tilfredsstillende retsmiddel i tilfælde af uenighed.

Fælles evaluering

Den årlige, fælles evalueringsmekanisme, der er nævnt i udkastet til tilstrækkelighedsafgørelsen, er en nøglefaktor i den overordnede troværdighed for værnet om privatlivets fred, og WP29 bifalder i høj grad den mulighed, som dette præsenterer for evalueringen af tilstrækkelighedsafgørelsen. I den henseende forstår WP29, at WP29's nationale repræsentanter vil kunne deltage fuldt ud i evalueringsprocessen, men beder om afklaring af de præcise arrangementer. Modaliteterne (inklusive den deraf følgende rapport, dens pr og de mulige konsekvenser, samt finansieringen) skal være aftalt i god tid forud for den første evaluering.

Konklusion

WP29 anfører de vigtige forbedringer, som værnet om privatlivets fred tilbyder sammenlignet med den ugyldiggjorte Safe Harbour-afgørelse. I lyset af de bekymringer, der er givet udtryk for, og de afklaringer, der bedes om, tilskynder WP29 Kommissionen til at løse disse bekymringer, identificere passende løsninger og fremsætte de anmodede afklaringer for at forbedre udkastet til tilstrækkelighedsafgørelsen og sikre, at den beskyttelse, der ydes af værnet om privatlivets fred, praktisk talt er tilsvarende til den i EU.

INDHOLDSFORTEGNELSE

1. INDLEDNING

Efter kendelsen afsagt af Den Europæiske Unions Domstol (i det følgende benævnt: EU-Domstolen) den 6. oktober 2015 i Schrems-sagen[1] opfordrede artikel 29-arbejdsgruppen (i det følgende benævnt: WP29, arbejdsgruppen) medlemsstaterne i Den Europæiske Union (i det følgende benævnt: EU) og de andre europæiske institutioner til åbne diskussioner med USA's myndigheder for at finde politiske, retslige og tekniske løsninger, der gør videregivelser til amerikanske områder, som respekterer grundlæggende rettigheder, mulige.

Den 2. februar 2016, efter mere end to års forhandlinger, nåede Europa-Kommissionen og det amerikanske handelsministerium til politisk enighed om en *ny ramme for transatlantiske udvekslinger af persondata til kommercielle formål: EU's og USA's værn om privatlivets fred* (i det følgende benævnt: værnet om privatlivets fred), som har til hensigt at erstatte USA's tidligere Safe Harbour.

Den 29. februar 2016 publicerede Kommissionen en meddelelse[2], et udkast til en tilstrækkelighedsafgørelse og de vedhæftede tekster, der vil udgøre værnet om privatlivets fred. I henhold til artikel 30, stk. 1, litra c), i direktiv 95/46/EF (i det følgende benævnt: direktivet) har WP29 vurderet disse dokumenter for at komme med sin aktuelle udtalelse om udkastet til tilstrækkelighedsafgørelsen, der udarbejdes af Kommissionen, inklusive de grundlæggende dokumenter for værnet om privatlivets fred. Under sin evaluering har WP29 inddelt arbejdet mellem en vurdering af den kommercielle del af værnet om privatlivets fred og en analyse af de sikkerhedsforanstaltninger, der er iværksat, hvad angår undtagelsesbestemmelserne for værnet om privatlivets fred til formål for national sikkerhed, retshåndhævelse og offentlige interesser.

Efter dommen i Schrems-sagen har WP29 afholdt flere møder med delegeringer fra den amerikanske regering, repræsentanter for civilsamfundsorganisationer fra både EU og USA samt videnskabsmænd for at udarbejde vurderingen af konsekvenserne ved dommen i Schrems-sagen. Under vurderingen af værnet om privatlivets fred har der været afholdt yderligere møder med Europa-Kommissionen og repræsentanter for den amerikanske regering. Under disse møder blev der fremsat nogle afklaringer, som der også er taget højde for i denne udtalelse. WP29 understreger, at disse afklaringer, på dette tidspunkt, kun er uformelle, og at de ikke kan betragtes som en integrerende del af udkastet til tilstrækkelighedsafgørelsen, da de endnu ikke er skrevet ned.

Ikke desto mindre bifalder WP29 især det engagement, som det amerikanske handelsministerium udviste under disse møder i forbindelse med samarbejde med databeskyttelsesmyndighederne i EU-medlemsstaterne, hvad angår anvendelsen af værnet om privatlivets fred, og at fremsætte vejledninger og retslig fortolkning, hvad angår anvendelsen af værnet om privatlivets fred, der skal publiceres på deres websteder.

[1] Sagen C-362/14 - Maximilian Schrems mod Data Protection Commissioner, 6. oktober 2015 (i det følgende benævnt: Schrems).
[2] COM(2016) 117 final af 29.2.2016.

1.1 Generelle bemærkninger

1.1.1 Anvendelsesområdet for WP29's vurdering

WP29 tog for det første højde for den gældende databeskyttelsesramme i medlemsstaterne i Den Europæiske Union, inklusive artikel 8 i den europæiske menneskerettighedskonvention (i det følgende benævnt: ECHR), der beskytter retten til privatliv og familieliv, samt artikel 7, 8 og 47 i EU's charter om grundlæggende rettigheder (i det følgende benævnt: charteret), der henholdsvis beskytter retten til privatliv og familieliv, retten til beskyttelse af persondata og retten til et effektiv retsmiddel og retfærdig rettergang. Den tog også højde for den relevante retslære samt direktivets krav.

Kravene til et tredjeland om at sikre et passende niveau for databeskyttelse blev yderligere defineret af EU-Domstolen i Schrems-sagen. Ikke alene forklarede domstolen, at direktivets bestemmelser skal tolkes "under hensyntagen til de grundlæggende rettigheder, som er sikret ved charteret"[3] og især artikel 7 og 8. Den angav også, at formuleringen "tilstrækkeligt beskyttelsesniveau" skal forstås således, at "det opstiller et krav om, at dette tredjeland på grundlag af dets nationale lovgivning eller dets internationale forpligtelser faktisk sikrer et beskyttelsesniveau for frihedsrettighederne og de grundlæggende rettigheder, som i det væsentlige svarer til det niveau, der er sikret inden for Unionen i medfør af direktivet, sammenholdt med chartret"[4]. Der er aldrig blevet foretaget en sådan vurdering med et tilstrækkeligt oplysningsniveau af den tidligere Safe Harbour-afgørelse. WP29 vurderer derfor udkastet til tilstrækkelighedsafgørelsen set i lyset af kravet om at fremsætte en analyse af beskyttelsesniveauet for grundlæggende rettigheder og friheder, der *praktisk talt svarer* til det niveau, der garanteres inden for EU. WP29 understreger, at denne udtalelse indeholder dens primære bekymringer, men at der i forbindelse med den begrænsede tid, der er gået, siden udkastet til tilstrækkelighedsafgørelsen blev publiceret, kan findes yderligere problemer på et senere tidspunkt.

WP29 anerkender, at ved at definere ordet "tilstrækkelig" i artikel 25, stk. 6, i direktivet som "praktisk talt svarende til", beskrev EU-Domstolen tilstrækkelighed yderligere i Schrems-sagen. Domstolen har understreget, at begrebet "tilstrækkeligt beskyttelsesniveau", selvom det ikke pålægger tredjelandet at sikre et beskyttelsesniveau, der er identisk til det niveau, der garanteres i den retslige kendelse i EU, skal forstås som "rent faktisk pålægger tredjelandet, som følge af dets indenrigslov eller dets internationale forpligtelser, at sikre et beskyttelsesniveau for grundlæggende rettigheder og friheder, der *praktisk talt svarer* til det, der garanteres inden for Den Europæiske Union i kraft af direktivet læst i relation til charteret".

1.1.2 Vurderingen af den kommercielle del af udkastet til tilstrækkelighedsafgørelsen

WP29 har allerede forklaret, hvordan EU's centrale databeskyttelsesprincipper for videregivelse af persondata til tredjelande ligger til grund for gruppens arbejdsdokument 12

[3] Schrems, §38.
[4] Schrems, §73.

"Videregivelse af personoplysninger til tredjelande: Anvendelse af artikel 25 og 26 i EU's databeskyttelsesdirektiv"[5]. WP29 har forsøgt at finde tilsvarende sikkerhedsforanstaltninger, som sikrer et beskyttelsesniveau, der svarer til de principper, der garanteres i direktivet, især vedrørende formålsbegrænsning, datakvalitet og -proportionalitet, gennemsigtighed, sikkerhed, aktindsigt, rettelse og modstand, dataopbevaring og begrænsninger for videregivelser. En lignende metode er blevet brugt i udtalelserne udstedt af WP29 på tidspunktet for vurderingen af den originale Safe Harbour-tilstrækkelighedsafgørelse[6], samt i anbefalinger fremsat af arbejdsgruppen i dennes brev til den tidligere vicepræsident og EU-justitskommissær Viviane Reding, publiceret den 10. april 2014[7].

1.1.3 Vurderingen af undtagelsesbestemmelser for offentlige myndigheders aktindsigt og deres sikkerhedsforanstaltninger

Vurderingen af undtagelsesbestemmelserne for offentlige myndigheders aktindsigt, der er dækket af værnet om privatlivets fred, er kompleks, især når der tages hensyn til databeskyttelsesmyndighedernes og offentlighedens skærpede bevidsthed om amerikanske overvågningsprogrammer efter Snowden-afsløringerne. Arbejdsgruppen anerkender og bifalder den amerikanske regerings indsats for at øge gennemsigtigheden af overvågningsprogrammer og deres villighed til at inkludere yderligere sikkerhedsforanstaltninger i værnet om privatlivets fred. Samtidig understreger WP29, at ethvert indgreb i de grundlæggende rettigheder for privatlivets fred og databeskyttelse skal kunne forsvares i et demokratisk samfund. EU-Domstolen kritiserede det faktum, at Safe Harbour-afgørelsen ikke indeholdt nogen konklusioner vedrørende eksistensen, i USA, af regler, der er indført af staten, og som har til hensigt at begrænse alle indgreb. Den henviser heller ikke til eksistensen af effektiv retslig beskyttelse mod nogen form for indgreb[8].

Derfor har WP29 analyseret den aktuelle amerikanske retslige ramme og amerikanske efterretningsbureauers fremgangsmetoder, som de er beskrevet i bilagene til udkastet til afgørelse, samt de betingelser, hvorunder de tillader indgreb i de grundlæggende rettigheder med respekt for privatlivets fred og for databeskyttelse som beskyttet under den europæiske retslige ramme.

For at evaluere, om noget indgreb kunne forsvares i et demokratisk samfund, blev vurderingen foretaget i relation til den europæiske retslære om grundlæggende rettigheder, som fastsætter fire essentielle garantier[9] for efterretningsaktiviteter:

A. Behandling bør ske i overensstemmelse med loven og baseret på klare, præcise og forståelige regler: Dette betyder, at alle, som er rimeligt informerede, bør være i stand

[5] Indført af WP29 den 24. juli 1998, se især side 6.
[6] Se WP62, WP32, WP27, WP23, WP21, WP19, WP15 og WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems, §§87, 88.
[9] De europæiske essentielle garantier er baseret på EU-Domstolens og ECtHR's retslære og er anført mere detaljeret i WP29 arbejdsdokumentet WP237, publiceret den 13. april 2016.

til at forudse, hvad der eventuelt kan ske med vedkommendes data der, hvor de bliver videregivet til.

B. Nødvendighed og proportionalitet, hvad angår de tilstræbte lovmæssige formål, skal påvises: Der skal findes en balance mellem formålene, hvortil dataene indsamles og tilgås og den fysiske persons rettigheder.
C. Der skal eksistere en uafhængig tilsynsmekanisme, som er både effektiv og upartisk: Det kan enten være en dommer eller anden uafhængig instans, så længe den er tilstrækkeligt i stand til at foretage de nødvendige tjek.
D. Effektive retsmidler skal være tilgængelige for den fysiske person: Alle skal have ret til at forsvare sine rettigheder foran en uafhængig instans.

1.2 Udkastet til tilstrækkelighedsafgørelsen

WP29 bifalder først og fremmest den kendsgerning, at en ny tilstrækkelighedsprocedure kan lanceres mindre end seks måneder efter, at EU-Domstolen erklærede Safe Harbour-afgørelsen for ugyldig. I lyset af den mængde dataoverførsler, der finder sted mellem EU og USA hver dag, hvilket WP29 anerkender som en afgørende del af økonomien på begge sider af Atlanterhavet, er der behov for retslig afklaring med det samme.

WP29 beklager imidlertid, at udkastet til tilstrækkelighedsafgørelsen, der er fremlagt af Kommissionen, ikke indeholder en omfattende vurdering af USA's indenrigslovgivning og internationale forpligtelser i form af en tilstrækkelighedsrapport, som tidligere har været almen praksis i lignende procedurer og i overensstemmelse med artikel 25 i direktivet. Dette har forhindret WP29 i at foretage en komplet analyse af den retslige kontekst, hvori værnet om privatlivets fred vil blive anvendt. Den anfører for eksempel, at det aktuelle udkast til tilstrækkelighedsafgørelsen hverken indeholder konklusioner vedrørende den lovgivning for privatlivets fred og databeskyttelse, der eksisterer i USA, både på føderalt og delstatsniveau, inklusive sektorspecifik lovgivning, eller nogen lovgivning, der tager ikke-overvågningsrelaterede former for offentlig aktindsigt i betragtning. Forholdet mellem dataoverførsler under værnet om privatlivets fred og under andre eksisterende tilstrækkelighedskonklusioner, såsom aftalen om passagerlisteoplysninger (PNR) og aftalen om Terrorist Finance Tracking Program (TFTP) mellem EU og USA, er heller ikke defineret.

1.2.1 Anvendelsesområdet for databeskyttelsesrammen i EU og især principperne i direktiv 95/46/EF

WP29 minder om, at under den retslige ramme for databeskyttelse i EU, især under direktivet (artikel 4, stk. 1), gælder medlemsstaternes love ikke kun for behandlingsprocessen, der foretages af dataansvarlige, der er veletablerede i deres område, men også hvor dataansvarlige (selvom de ikke er veletablerede i EU) gør brug af udstyr, der befinder sig i et europæisk område, især til indsamlingen af persondata. Som konsekvens gælder EU-medlemsstatens lov for al behandling, der finder sted inden videregivelsen til USA, enten i forbindelse med en organisation, der er veletableret i EU, eller via brug af udstyr, der befinder sig i EU, der bruges af en organisation, som ikke er veletableret i EU. WP29 anmoder om, at dette gøres tydeligt i udkastet til tilstrækkelighedsafgørelsen.

Det skal være klart, at principperne for værnet om privatlivets fred vil være gældende fra det øjeblik, dataoverførslen finder sted. WP29 minder desuden om, at dataansvarlige, der er veletablerede i EU, og som videregiver data til en databehandler i USA, forbliver underlagt EU's databeskyttelseslovgivning.

1.2.2 Mangel på klarhed i dokumenterne til værnet om privatlivets fred

Det faktum, at de principper og garantier, der gives af værnet om privatlivets fred, er fremsat i både tilstrækkelighedsafgørelsen og i dens bilag, gør informationen både vanskelig at finde og, til tider, selvmodsigende. Dette bidrager til en samlet mangel på klarhed i forbindelse med den nye ramme samt gør tilgængeligheden for registrerede, organisationer og databeskyttelsesmyndigheder vanskeligere. Ligeledes mangler det anvendte sprog klarhed. Derfor opfordrer WP29 Kommissionen til at gøre dette klart og forståeligt for begge sider af Atlanterhavet.

WP29 foreslår at inkludere et separat bilag, der fremsætter definerede kernebegreber, som bruges i dokumenterne til værnet om privatlivets fred. En almindelig og utvetydig forståelse for forpligtelserne, der pålægges af tilstrækkelighedsafgørelsen i forbindelse med værnet om privatlivets fred, er afgørende for dens effektive funktion på begge sider af Atlanterhavet, og som sådan er WP29 bekymret over, at der som følge af adskillige henvisninger og ikke-afstemte formuleringer samt kompleksiteten ved rammedokumenterne vil opstå problemer i forbindelse med overensstemmelsen, forståeligheden og klarheden af implementeringen af værnet om privatlivets fred.

Endnu vigtigere gør dokumenterne til værnet om privatlivets fred brug af terminologi, der ikke er konsistent med det ordforråd, der almindeligvist bruges i EU i forbindelse med databeskyttelse. Det er ikke nødvendigvis et problem, så længe det står klart, hvad den tilsvarende terminologi ifølge EU-lovgivning (og ifølge amerikansk lov) ville være. WP29 beklager imidlertid at måtte anføre, at det ikke er tilfældet, inklusive i udkastet til tilstrækkelighedsafgørelsen. For eksempel bruges ordet "aktindsigt" i kapitel 3 i udkastet til tilstrækkelighedsafgørelsen på en måde, der indikerer indsamlingen af persondata fremfor at tillade en person at se data, der allerede er indsamlet. Virksomheders og de fysiske personers aktindsigt er to separate begreb, der ikke bør forveksles.

WP29 understreger, at terminologien også skal bruges konsekvent i alle dokumenterne, inklusive i udkastet til tilstrækkelighedsafgørelsen. Dette er aktuelt ikke tilfældet, for eksempel for begreberne "behandling" og "persondata". Begge er i princippet veldefinerede i Bilag II, men ikke konsekvent anvendt i dokumenterne, hvilket resulterer i smuthuller i beskyttelsen[10,11].

[10] Nogle af bestemmelserne nævner udelukkende nogle former for databehandlingsaktiviteter i stedet for at gøre brug af begrebet "behandling". Dette resulterer i smuthuller i beskyttelsen. F.eks. i henhold til formuleringen i Bilag II, III.6.f, ville principperne for værnet om privatlivets fred kun være gældende, hvor organisationen "opbevarer, bruger eller offentliggør" de modtagne data (dvs. ikke for andre aktiviteter, der er dækket af begrebet "behandling", såsom indsamling, registrering, ændring, hentning, rådgivning, sletning). Datasikkerhed ville kun blive pålagt "oprettelse, vedligeholdelse, brug eller udbredelse" af personlige oplysninger (Bilag II, II.4). Definitionen af persondata er også begrænset til data, der "modtages" og "registreres". Som endnu et eksempel fremsætter oplysningsprincippet (Bilag II, II.1.a.iv), at den certificerede

WP29 bifalder, at definitioner af nogle af de anvendte begreber har været inkluderet i de dokumenter, som udgør værnet om privatlivets fred. Dette er imidlertid ikke tilfældet for flere af de andre essentielle begreber, inklusive "agenter" eller "behandler", "nøglekodede data", "anonymiserede data" og "fysisk person i EU", som i lyset af WP29 garanterer en klar definition, hvor både USA og EU bliver enige om de tilsynsførende myndigheder og offentligheden for at undgå forvirring på et senere tidspunkt for både de dataansvarlige og -behandlerne, som anvender værnet om privatlivets fred. En nem løsning ville være at tilføje en ordliste til de Ofte stillede spørgsmål vedrørende værnet om privatlivets fred.

WP29 indikerer også de lovmæssige grundlag for behandling af følsomme data i tillægsprincip 1 (bilag II, III.1) i tilfælde, hvor en organisation ikke er nødsaget til at opnå udtrykkeligt samtykke (tilmelding). Dette tillægsprincip 1 kan forstås som en detaljeret beskrivelse af det lovmæssige grundlag for indsamlingen af data i EU, da denne liste svarer til artikel 8 i direktivet. WP29 ønsker at minde om, at al behandling (inklusive indsamling og videregivelse) af følsomme data underlagt EU-lovgivning skal ske på lovmæssige grundlag i henhold til artikel 8 i direktivet. Værnet om privatlivets fred kan ikke tolkes som en fremsættelse af alternative grundlag for sådan behandling. For eksempel er det ifølge WP29 ikke muligt for en amerikansk organisation at indsamle data underlagt EU-lovgivning på grundlag af amerikansk ansættelsesret (se bilag II, III.1.a.v). Derfor understreger WP29, at enhver tolkning af tillægsprincip 1 kun må føre til dets gyldighed for følsomme data, der allerede er videregivet, efter de er blevet indsamlet i EU på lovmæssige grundlag anført i artikel 8 i direktivet.

Endelig anfører WP29 en mangel på klarhed i forbindelse med spørgsmålet angående, hvem der kan betragtes som værende en fysisk person i EU og dermed drager fordel af beskyttelse under værnet om privatlivets fred: alle EU-borgere eller alle personer, der er bosiddende i EU. Dette er særligt vigtigt i forbindelse med retten til afhjælpning, inklusive adgangen til ombudspersonen. Tilstrækkelighedsafgørelsen skal endvidere anføre spørgsmålet vedrørende, i hvilken udstrækning værnet om privatlivets fred også vil gælde for borgere/bosiddende i landene i EØS og Schweiz, som tidligere var dækket af Safe Harbor-ordningen.

1.2.3 Fælles evaluering og suspension

WP29 bifalder det faktum, at Europa-Kommissionen og den amerikanske regering er blevet enige om regelmæssig evaluering af den praktiske anvendelse af værnet om privatlivets fred. Den fælles evaluering har været en kendt praksis i databeskyttelsessamfundet i EU i flere år, især i forbindelse med aftalerne om udveksling af PNR-data med tredjelande og TFTP-

organisation skal informere fysiske personer om de formål, hvortil den "indsamler og bruger" data om dem. Bilag II, III.9.a.11 nævner udelukkende data, der "videregives" eller "tilgås". Selvom det lader til, at hensigten i de fleste tilfælde ikke er at begrænse princippernes anvendelsesområde eller at skabe huller i beskyttelsen, medfører denne selvmodsigende terminologi risikoen for sådanne huller. Da begrebet "behandling" er defineret i principperne, er det afgørende at gøre brug heraf på en konsekvent måde for at undgå de nu eksisterende smuthuller. Ellers ville der være for meget spillerum til formentligt utilsigtet tolkning, som ellers kunne føre til fejlfortolkning af afgørelsens formulering.

[11] Definitionen af "persondata", som er inkluderet i Bilag II, I.8.a, henviser til "data om en identificeret eller identificerbar fysisk person". Tillægsprincippet fremsætter imidlertid, at hvad angår HR-data, gælder principperne kun, når "identificerede fortegnelser videregives eller tilgås". WP29 tager højde for, at dette åbner op for en mulighed for at behandle persondata på en måde, der hverken er i overensstemmelse med databeskyttelsesprincipperne ifølge EU-lovgivning eller med den generelle definition af persondata under værnet om privatlivets fred.

aftalen. WP29 bifalder endvidere det faktum, at et uspecificeret antal repræsentanter fra databeskyttelsesmyndigheder kan deltage i disse fælles evalueringer.

Set i lyset af dens erfaring med fælles evalueringer i de senere år ønsker WP29 at gøre det klart, at den forventer, at den fælles evaluering af værnet om privatlivets fred er mere omfattende end de fælles evalueringer af PNR og TFTP. Det ønskes især, at den fælles evaluering ikke blot vil omfatte møder med repræsentanter for amerikanske bureauer, organisationer og forretninger, men også lokale kontrolbesøg med henblik på kontrol af visses elementer i værnet om privatlivets fred. Databeskyttelsesmyndigheders repræsentanter i den fælles evaluering bør være i stand til at komme med forslag til sådanne verificeringer på stedet.

WP29 tager højde for, at en fælles evaluering kræver en fælles vurdering af konklusionerne. Hidtil er resultaterne af fælles evalueringer blevet præsenteret i et arbejdsdokument fra Kommissionens tjenestegrene, hvor godkendelse fra de medlemmer i den fælles evaluering, som ikke var fra Kommissionen, ikke var påkrævet. Til den fælles evaluering af værnet om privatlivets fred vil WP29 sætte pris på, hvis rapporten med konklusionerne rent faktisk kunne være et delt produkt. Alternativt kan offentliggørelsen af en separat fælles evalueringsrapport fra databeskyttelsesmyndigheden overvejes.

Endelig, hvad angår den fælles evaluering, minder WP29 om Kommissionens løfte om, at udgifter, som WP29-repræsentanterne har påløbet sig under fælles evalueringer, skal godtgøres af Kommissionen. Arbejdsgruppen formoder, at dette også vil gælde for den fælles evaluering af værnet om privatlivets fred, under alle omstændigheder for et rimeligt antal databeskyttelsesmyndigheders repræsentanter.

WP29 anbefaler, at man senest tre måneder inden udførelsen af den første fælles evaluering af værnet om privatlivets fred bliver enige om modaliteterne for den fælles evaluering mellem Kommissionen, den amerikanske regering og WP29, og at de registreres skriftligt.

1.2.4 Retslig ramme i EU under revidering

Tilstrækkelighedsafgørelsen vedrørende værnet om privatlivets fred er den første tilstrækkelighedsafgørelse, der er lavet udkast til efter den principielle aftale vedrørende teksten i den generelle databeskyttelsesforordning. WP29 har imidlertid konstateret, at værnet om privatlivets fred endnu ikke afspejler den fremtidige situation. For eksempel er vigtige nye begreber, såsom retten til datamobilitet og yderligere forpligtelser for dataansvarlige, inklusive behovet for at foretage vurderinger af vores databeskyttelses effekt og for at overholde de tilsigtede og standard principper for privatlivets fred, ikke blevet inkluderet i værnet om privatlivets fred. Derfor ønsker WP29 at foreslå, at værnet om privatlivets fred, som med alle eksisterende tilstrækkelighedsafgørelser, evalueres kort tid efter, at GDPR træder i kraft. En udtrykkelig henvisning til denne evalueringsproces i den endelige tilstrækkelighedsafgørelse vil være påskønnet.

2. VURDERING AF DEN KOMMERCIELLE DEL AF UDKASTET TIL TILSTRÆKKELIGHEDSAFGØRELSEN

2.1 Generelle bemærkninger

2.1.1 Forbedringer

WP29 bifalder de forbedringer, som værnet om privatlivets fred bringer, og dens forhandleres vilje til at forsøge at tage sig af de utilstrækkeligheder ved Safe Harbour, som er blevet understreget. Sammenlignet med Safe Harbour kan forbedringer især bemærkes for følgende elementer: indsættelsen af visse nøgledefinitioner såsom "persondata", "behandling" og "dataansvarlig", de mekanismer, der er oprettet for at sikre tilsynet med listen over værnet om privatlivets fred og de nu obligatoriske eksterne og interne overholdelsesevalueringer. Der er også foretaget forbedringer til indsigtsprincippet, og WP29 anfører, at der nu er givet ret til rettelse og sletning, når data anvendes på en måde, der er uforenelig med principperne for værnet om privatlivets fred. Endvidere gøres det nu klart, at den fysiske person skal modtage både bekræftelse på, at dataene vedrørende denne er under behandling, og meddelelse om de behandlede data.

WP29 bifalder også styrkelsen af de retslige garantier, hvor videregivelser finder sted, samt det amerikanske handelsministeriums og Federal Trade Commissions (FTC) forpligtelser til at styrke de forpligtelser, der er fremsat af værnet om privatlivets fred.

2.1.2 Anvendelse af værnet om privatlivets fred for organisationer, der fungerer som behandler (agent)

Den udstrækning, hvormed principperne for værnet om privatlivets fred er gældende for certificerede organisationer, der blot modtager persondata fra EU til behandlingsformål (henvist til som "agenter" eller "behandlere"), forbliver desværre stadig uklar. Selvom bestemmelserne i bilag II, III.10.a. nævner dataoverførsler til certificerede organisationer til sådanne formål - dvs. nævnelse af kravet om at indgå en kontrakt - mangler de en tilkendegivelse af, hvordan principperne for værnet om privatlivets fred skal gælde for behandlere (agenter). Dette skaber uvished, både for de certificerede amerikanske organisationer, der modtager data til behandlingsformål, og for EU-virksomheder, der foretager dataoverførsler til certificerede organisationer, der fungerer som databehandlere, samt for de fysiske personer, hvis data bliver behandlet. Derfor vil det være vanskeligt at fastslå, hvilke pligter der rent faktisk gælder for værnets organisationer, der behandler persondata, som modtages fra EU, i deres rolle som behandlere. Derfor er afklaring helt sikkert påkrævet.

Der skal tages højde for, at flere af forpligtelserne, der er indeholdt i principperne, ikke er egnet for databehandlere, da det altid er den dataansvarlige, der fastslår formålene for og metoderne til behandling af dataene (jf. definitionen af dataansvarlig i bilag II, I.8.c). Derfor kan nogle forpligtelser, der er indeholdt i principperne, hvis de gøres gældende for en organisation, der fungerer som agent, modsige databehandlingskontrakten, som er påkrævet i henhold til EU-lovgivningen (kontrakten, der er nævnt i bilag II, III.10.a.). For eksempel vil

databehandleren (agenten) ifølge databehandlingskontrakten generelt ikke kunne videregive data til en tredjepartsansvarlig, selv under de omstændigheder, der er nævnt i bilag II, II.3.a. Videregivelser til tredjepartsagenter bør kun autoriseres efter forudgående godkendelse af den dataansvarlige. I henhold til kravene i EU-lovgivningen vil en behandler (agent) heller ikke kunne give fysiske personer fulde oplysninger som tilsigtet af oplysningsprincippet (bilag II, II.1), for eksempel fordi denne organisation ikke fastslår behandlingsformålene.

Derfor er det afgørende at afklare i principperne, at i tilfælde af en sådan modsigelse vil bestemmelserne i databehandlingskontrakten og især vejledningen fra den organisation, der videregiver data ud af EU, gælde. Uden en sådan afklaring kan principperne tolkes og anvendes på en måde, der giver værnets agent for mange kontrolkapaciteter, og dette vil bringe EU-dataeksportøren i fare for at overtræde sine forpligtelser som dataansvarlig i henhold til EU's databeskyttelseslovgivning, som denne er underlagt, under videregivelse af data til en organisation under værnet, der fungerer som en agent. Denne mangel på klarhed giver endvidere indtrykket af, at behandleren eventuelt vil genbruge dataene, som han ønsker.

Der skal endvidere fremsættes specifikke regler, når en organisation fungerer som en databehandler (agent) for at sikre, at denne organisation respekterer den dataansvarliges vejledning. Det skal gøres klart, at amerikanske organisationer, der udelukkende modtager data til behandlingsformål, ikke kan beslutte at behandle dataene på egne vegne. Ved manglen på specifikke regler, der gælder for organisationer, der fungerer som behandler, er det vanskeligt at fastslå, ud fra hvilke regler behandleren (agenten) vil kunne certificere sig selv.

2.1.3 Begrænsninger for pligten til at overholde principperne

Bilag II, I.5. fremsætter blandt andet undtagelser fra principperne, når data, der er dækket af værnet om privatlivets fred, anvendes af årsager vedrørende[12], offentlig interesse, retshåndhævelse eller i overholdelse af vedtægt, regeringsbestemmelse eller retspraksis, der skaber modstridende forpligtelser eller udtrykkelige autorisationer. Uden fuldt kendskab til amerikansk lov på både føderalt og statsniveau, er det vanskeligt for WP29 at vurdere denne undtagelses anvendelsesområde og at overveje, om disse begrænsninger kan forsvares i et demokratisk samfund. Det ville være afgørende, at Europa-Kommissionen også inkluderer en analyse af beskyttelsesniveauet, hvor disse undtagelser ville være gældende, i sit udkast til tilstrækkelighedsafgørelsen. WP29 opfordrer Kommissionen til at sikre, at EU er informeret om alle vedtægter eller regeringsbestemmelser, som ville påvirke overholdelsen af principperne, som enten er aktuelt gældende, eller på det tidspunkt, hvor nye vedtægter eller bestemmelser træder i kraft i USA.

2.1.4. Mangel på et princip for begrænsning af dataopbevaring

Princippet om begrænsning af dataopbevaring (artikel 6, stk. 1, litra e), i direktivet) er et grundlæggende princip i EU's databeskyttelseslovgivning, der pålægger, at persondata kun må

[12] Se kapitel 3 for yderligere kommentarer vedrørende brugen af persondata, der er dækket af værnet om privatlivets fred til formål for national sikkerhed, og kapitel 4 for retshåndhævelsesformål.

gemmes så længe, det er nødvendigt for at opnå det formål, hvortil dataene blev indsamlet, eller hvortil de bliver yderligere behandlet.

WP29 kan imidlertid ikke finde nogen henvisning til nødvendigheden for, at dataansvarlige sikrer, at dataene slettes, når først formålet, hvortil de blev indsamlet eller yderligere behandlet, er blevet forældet, i dokumenterne, der udgør værnet om privatlivets fred. Som det ser ud, pålægger principperne derfor ikke de certificerede organisationer en grænse for opbevaringsperioden for dataene tilsvarende det, der pålægges af princippet om begrænsning af dataopbevaring i henhold til EU-lovgivningen.

Formuleringen i princippet om dataintegritet og formålsbegrænsning (bilag II, II.5) kan på ingen måde betragtes som oprettelse af en forpligtelse for en organisation, der fungerer som en dataansvarlig, om at slette data, når de ikke længere er nødvendige til de formål, hvortil de er blevet indsamlet eller yderligere behandlet, eller for en organisation, der fungerer som en behandler, om at slette data efter serviceaftalens ophør.

Arbejdsgruppen understreger, at manglen på bestemmelser, der indfører en grænse for opbevaring af data under værnet om privatlivets fred, giver organisationer mulighed for at gemme data så længe, de ønsker, selv efter de har forladt værnet om privatlivets fred, hvilket ikke er på linje med princippet om begrænsning af dataopbevaring.

2.1.5 Mangel på garantier for automatiserede beslutninger, som har retsvirkning for, eller som berører den fysiske person i væsentlig grad

Værnet om privatlivets fred fremsætter ingen retslige garantier, hvor fysiske personer er undergivet afgørelser, der har retsvirkning for dem, eller som berører dem i væsentlig grad, og som alene er truffet på grundlag af edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom erhvervsevne, kreditværdighed, pålidelighed, adfærd osv.

Nødvendigheden for at fremsætte retslige garantier for automatiserede beslutninger (der har retsvirkning for, eller som berører den fysiske person i væsentlig grad**)** for at give et tilstrækkeligt beskyttelsesniveau er allerede blevet fremhævet af WP29 i dens arbejdsdokument 12.

Nødvendigheden bliver endnu mere afgørende, da den evige udvikling af nye teknologier gør flere virksomheder i stand til at overveje implementeringen af systemer til automatiseret beslutningstagning, som kan føre til en svækkelse af positionen for de fysiske personer, der står tilbage uden nogen regres mod de computergenererede beslutninger. Hvor beslutninger, som udelukkende er taget af disse edb-systemer, berører de fysiske personers retslige situation eller berører dem i væsentlig grad (for eksempel ved at sortliste og dermed fratage de fysiske personer deres rettigheder), er det afgørende at fremsætte tilstrækkelige sikkerhedsforanstaltninger, inklusive retten til at kende den involverede logik og til at anmode om genovervejelse på et ikke-automatiseret grundlag.

2.1.6 Midlertidig periode for eksisterende kommercielle relationer

Værnet om privatlivets fred forudser, at principperne gælder umiddelbart efter certificering. Organisationer, der vil certificere inden for de to første måneder efter ikrafttrædelsesdatoen for rammen for værnet om privatlivets fred, skal gøre alle eksisterende kommercielle relationer med tredjeparter overensstemmende med princippet om ansvarlighed for videregivelse så hurtigt som muligt. Under alle omstændigheder skal de senest gøre det ni måneder fra den dato, hvor de certificeres til værnet om privatlivets fred.

Det betyder, at eksisterende kontrakter i det nødvendige omfang skal bringes på linje med principperne mellem to og ni måneder efter certificering. Under denne midlertidige periode er oplysning og valg tilstrækkeligt. WP29 kræver, at ud fra det faktum, at videregivelser kun kan finde sted på grundlag af værnet om privatlivets fred fra det øjeblik, hvor organisationen kan overholde alle kravene for værnet fuldt ud. En mulighed for at sende data under en midlertidig periode, uden at modtageren er i stand til fuldt ud at overholde værnets principper, kan ikke anses for at overholde betingelserne for en retslig videregivelse og er derfor ikke acceptabel.

2.2 Specifikke bemærkninger

2.2.1 Gennemsigtighed

a) Oplyste generelle bemærkninger

WP29 bifalder de mere omfattende og detaljerede krav, som er fremsat under oplysningsprincippet, især at oplysningen vil skulle indeholde et link til eller en webadresse på listen over værnet om privatlivets fred og henvise til fysiske personers aktindsigt samt de alternative stridsløsningsmekanismer[13]. WP29 foreslår imidlertid at være mere tydelig, hvad angår andre dækkede rettigheder (til at rette, slette, hvor data er unøjagtige eller behandlet i strid med principperne).

Dokumenterne, der udgør værnet om privatlivets fred, giver anledning til bekymring, hvad angår det tidspunkt, hvor en organisation under værnet om privatlivets fred skal oplyse en fysisk person. Bilag II, II.1.b fremsætter, at "oplysningen skal formidles (...), når fysiske personer første gang anmodes om at levere personoplysninger til organisationen, eller så hurtigt som muligt derefter, dog under alle omstændigheder inden organisationen anvender sådanne oplysninger til et andet formål end det, hvortil de oprindeligt blev indsamlet eller behandlet af det foretagende, der har videregivet oplysningerne, eller videregiver dem for første gang til tredjepart". WP29 tager højde for, at i mange situationer vil organisation under det amerikanske værn ikke direkte indsamle data fra registrerede, og derfor skal tidspunktet for oplysningen være på det tidspunkt, hvor dataene registreres af værnsorganisationen.

[13] Bilag II, II.1; WP29 henviser også til den anden af Kommissionens anbefalinger, som blev fremsat i meddelelsen COM(2103)847 samt WP29's brev til næstformand Viviane Reding dateret 10. april 2014, især punkt 4 under "Gennemsigtighed".

WP29 anfører, at den faktiske implementering af kravene, hvad angår oplysningsprincippet og politikken om privatlivets fred, skal vurderes ved den første årlige evaluering af værnet om privatlivets fred.

b) Offentlig tilgængelighed af politikken om privatlivets fred

WP29 bifalder det faktum, at det nu er tydeligt, at det amerikanske handelsministerium vil kontrollere, om virksomheder, der har offentlige websteder, har offentliggjort deres politik om privatlivets fred på dette websted, eller, hvis de ikke har nogen offentlige websteder, hvor politikken om privatlivets fred er gjort tilgængelig for offentligheden[14].

c) Publicering af betingelser for privatlivets fred, hvad angår kontrakter med behandlere

Værnet om privatlivets fred fremsætter blandt betingelserne, hvorunder organisationer under værnet om privatlivets fred kan videregive data til en behandler (agent), en forpligtelse til selvcertificerede organisationer om at "fremsætte et resumé eller en repræsentativ kopi af de relevante bestemmelser for privatlivets fred i dets kontrakt med den agent til ministeriet efter anmodning" (se bilag II, II. 3.b.v). Arbejdsgruppen bifalder dette gennemsigtighedskrav for det amerikanske handelsministerium.

2.2.2 Valg

Værnet om privatlivets fred fremsætter en ret til at framelde offentliggørelse af personlige oplysninger til en tredjepart eller til brugen af personlige oplysninger til et formål, der er væsentligt anderledes[15] (bilag II, III, 2). Fysiske personer nyder endvidere godt af en ret til at "framelde" brugen af personlige oplysninger til direkte markedsføringsformål når som helst (bilag II, III.12.a)[16].

Med undtagelse af konteksten af direkte markedsføringsformål er der ikke fremsat nogen oplysninger om måden hvorpå, og tidspunktet hvor, denne framelding kan udøves. WP29 tager højde for, at den simple henvisning til denne rets eksistens i politikken om privatlivets fred ikke kan være tilstrækkelig, men en *individuel* mulighed for at udøve denne ret skal tilbydes *inden* offentliggørelsen eller genanvendelsen af personlige oplysninger.

Endvidere understreger WP29, at en generel ret til at fremsætte indsigelser (på tungtvejende grundlag vedrørende den registreredes særlige situation), der forstås som en ret til at bede om at standse behandlingen af ens data, når den fysiske person har tungtvejende grundlag vedrørende vedkommendes særligt situation, skal tilbydes inden for værnet om privatlivets fred[17]. WP29 anbefaler på det kraftigste, at udkastet til tilstrækkelighedsafgørelsen gør det

[14] Se den første anbefaling fremsat af Europa-Kommissionen i dennes meddelelse COM(2013)847 og WP29's brev til næstformand Viviane Reding dateret 10. april 2014, især punkt 3 under "Gennemsigtighed"
[15] Tillægsprincippet 14.c.I fremsætter retten til at trække sig tilbage fra et klinisk forsøg, som eventuelt kan ses som retten til at fremsætte indsigelser eller til at trække samtykke tilbage.
[16] Det er identisk til det, der er fremsat i Safe Harbour-ordningen (Ofte stillede spørgsmål 12), og der er ikke foretaget nogen ændringer desangående.

klart, at retten til at fremsætte indsigelser bør eksistere på et givet tidspunkt, og at denne indsigelse ikke er begrænset til brugen af dataene til direkte markedsføring[18].

WP29 frygter, at manglen på definition af det, der skal anses som et "væsentligt anderledes" formål, vil føre til forvirring og retslig usikkerhed. Det skal klargøres, at valgprincippet under alle omstændigheder ikke kan bruges til at omgå princippet om formålsbegrænsning[19]. Valg skal kun være tilgængeligt, hvor formålet er væsentligt anderledes, men stadig forenelig, da behandlingen for uforenelige formål er forbudt (bilag II, II.5.a). Det skal klargøres, at retten til framelding ikke kan gøre organisationen i stand til at bruge data til uforenelige formål. Derfor anbefales det at harmonisere den relaterede formulering ved hjælp af en enkel og defineret formulering (f.eks. "væsentligt anderledes, men stadig foreneligt formål").

Afklaring vil være nyttig, hvad angår, når en beslutning, der tages om at behandle data til et andet formål eller til at offentliggøre oplysninger, falder ind under EU-lovgivning. I denne situation vil de sædvanlige retslige betingelser vedrørende denne behandling (såsom forbuddet mod behandling til uforenelige formål, at fremsætte et lovmæssigt grundlag for behandlingen og behovet for at informere den fysiske person) være direkte gældende, inklusive for den amerikanske organisation, der falder ind under anvendelsesområdet for EU-lovgivning. I praksis betyder det, at det vil være op til EU-eksportøren, der tager en sådan beslutning, at sikre gennemsigtighed og retmæssighed for behandlingen i henhold til EU-lovgivning. Derfor gælder valgprincippet kun, hvor beslutningen udelukkende tages af den amerikanske organisation ikke underlagt EU-lovgivning.

2.2.3 Videregivelser

a) Anvendelsesområde

WP29 er bekymret over den situation, hvor videregivelser af persondata finder sted fra en organisation, der er certificeret under værnet om privatlivets fred i USA, til en modtager i et tredjeland.

Værnet skal ikke kun ses som et værktøj til at videregive EU-data fra EU til USA, men vil også fungere som et værktøj, der skal bruges til at videregive data fra USA til tredjelande. Derfor er bestemmelser for videregivelser et vigtigt element for værnet, der skal fremsætte tilstrækkelige garantier og et tilstrækkeligt beskyttelsesniveau, når data videregives uden for USA. Et særligt problem er forbundet med national sikkerhed og retshåndhævelse.

Princippet om ansvarlighed for videregivelse i forbindelse med værnet om privatlivets fred er ikke begrænset til modtagerens dataansvarlige, behandlere eller agenter, der er veletablerede i USA. Derfor kan videregivelser til et tredjeland finde sted på grundlag af værnet om privatlivets fred, selv hvis tredjelandet har love, der giver aktindsigt til for eksempel overvågningsformål. Dette bringer EU-data i fare for ubegrundede indgreb med beskyttelsen af de grundlæggende rettigheder.

[18] Se WP29's brev til næstformand Viviane Reding under "Valg".
[19] Et konkret eksempel på yderligere uforenelig behandling, der er autoriseret under valgprincippet, er fremsat under tillægsprincippet 9.b.i (se WP29-bemærkningen herom under punktet, der vedrører "HR-data").

I tilfælde af en videregivelse til et tredjeland skal alle organisationer under værnet om privatlivets fred være forpligtet til at vurdere alle obligatoriske krav for tredjelandets nationale lovgivning, der er gældende for dataimportøren, forud for videregivelsen. Hvis der identificeres en væsentlig, ufordelagtig virkning på garantierne, forpligtelserne og beskyttelsesniveauet, der tilvejebringes af værnet om privatlivets fred, skal den amerikanske organisation under værnet om privatlivets fred, der fungerer som en behandler (agent), omgående underrette den dataansvarlige i EU, inden der foretages en videregivelse. I disse tilfælde er dataeksportøren berettiget til at suspendere dataoverførslen og/eller opsige kontrakten. Hvor der er en sådan fare for en væsentlig, ufordelagtig virkning, må en værnorganisation, der fungerer som en dataansvarlig, ikke videregive data, da det vil kompromittere dens pligt til at yde samme beskyttelsesniveau som under principperne i tilfælde af videregivelser (se bilag II, II.3.a).

I tilfælde af en ændring i tredjelandets lovgivning, som sandsynligvis vil have en væsentlig, ufordelagtig virkning på garantierne, forpligtelserne og beskyttelsesniveauet, der tilvejebringes af værnet om privatlivets fred, skal den amerikanske organisation under værnet om privatlivets fred, der fungerer som en behandler (agent), ligeledes være forpligtet – af værnet om privatlivets fred – til omgående at meddele denne ændring til dataeksportøren så snart, den får kendskab hertil, og i det tilfælde er dataeksportøren berettiget til at suspendere videregivelsen af data og/eller opsige kontrakten. I et sådan tilfælde må en værnorganisation, der fungerer som en dataansvarlig, ligeledes ikke videregive data, da det vil kompromittere dens pligt til at yde samme beskyttelsesniveau som under principperne (se bilag II, II.3.a).

WP29 minder om sin position, hvis den dataansvarlige i EU er bekendt med en videregivelse til en tredjepart uden for USA, selv inden videregivelse til USA finder sted, eller hvis den dataansvarlige i EU har fælles ansvar for beslutningen om at tillade videregivelser, skal videregivelsen betragtes som en direkte videregivelse fra EU til tredjelandet uden for USA. Det betyder, at artikel 25 og 26 i direktivet gælder for videregivelsen i stedet for princippet om videregivelse under værnet om privatlivets fred.

b) Videregivelser fra en organisation under værnet om privatlivets fred til en tredjeparts dataansvarlige

WP29 bifalder pligten til at få kontrakter på plads (bilag II, II.3.a) for at sikre, at en tredjeparts dataansvarlige vil yde mindst samme beskyttelsesniveau for privatlivets fred som påkrævet af principperne for værnet om privatlivets fred. Formålet er at sikre, at persondata fortsat er tilstrækkeligt beskyttet, selv efter at være blevet videregivet. WP29 har imidlertid nogle bemærkninger til de foreslåede betingelser.

<u>Mangel på henvisning til princippet om formålsbegrænsning</u>

WP29 anbefaler også at indsætte en klar henvisning til princippet om formålsbegrænsning (bilag II, II.5) inden for betingelserne for videregivelser til en tredjeparts dataansvarlige (bilag II, II.3.a). Dette vil gøre det klart, at videregivelser ikke må finde sted, hvor tredjepartens dataansvarlige vil behandle data til et uforeneligt formål.

Undtagelse af behovet for kontrakt for intragruppevideregivelser mellem dataansvarlige

En undtagelse af behovet for kontrakt er fremsat for intragruppevideregivelser mellem dataansvarlige. I et sådant scenarie anfører principperne, at beskyttelseskontinuiteten kan tilbydes af Binding Corporate Rules (BCR'er) eller "andre intragruppeinstrumenter" (f.eks. overholdelse og kontrolprogrammer)" (bilag II, III.10.b). WP29 tager højde for, at henvisningen til "andre intragruppeinstrumenter" ikke garanterer juridisk bindende forpligtelser fremsat af andre af gruppens medlemmer. Da WP29 og EU-lovgivningen[20] generelt favoriserer bindende forpligtelser med at formulere intragruppevideregivelser, er det vigtigt at undgå, at værnet om privatlivets fred bruges på en måde, der skal omgå dette krav. WP29 minder om, at videregivelser fra USA til tredjelande, der allerede blev planlagt inden videregivelsen til USA finder sted, eller som er underlagt fælles kontrol med den dataansvarlige i EU[21] under alle omstændinger skal anses som en direkte videregivelse fra EU til tredjelandet uden for USA. Derfor er artikel 25 og 26 i direktivet gældende for videregivelsen.

c) Videregivelser fra en organisation under værnet om privatlivets fred til en tredjeparts behandler (agent)

WP29 bifalder det faktum, at en kontrakt for videregivelser nu er obligatorisk for modtagende entiteter, der fungerer som behandlere (agenter) uanset deres deltagelse i værnet om privatlivets fred, eller hvis de drager fordel af en anden løsning til at opnå tilstrækkelighed. WP29 bifalder også de yderligere sikkerhedsforanstaltninger, der sætter ramme om disse videregivelser (bilag II, II.3.a.i; II.3.a.iii; II.3.a.iv; II.3.a.v; II.7.d). Det sidste punkt (bilag II, II.7.d) vedrører forpligtelsen til at forblive ansvarlig, når data offentliggøres over for en agent. Det lader imidlertid til, at denne garanti ikke vil gælde, hvis en organisation har valgt at samarbejde med en databeskyttelsesmyndighed (se bilag II, III.5.a opsummeret). WP29 forstår ikke årsagen til en sådan undtagelse og mener, at ansvar skal gælde selv i dette tilfælde.

Mangel på henvisning til princippet om formålsbegrænsning

WP29 anfører, at princippet om ansvarlighed for videregivelse (bilag II, II.3) forklarer, at persondata kun kan videregives til en tredjepart, der fungerer som en agent, til begrundede og præciserede formål, men siger ikke udtrykkeligt, at disse begrænsede og præciserede formål skal være forenelige med de første formål, hvortil dataene blev indsamlet, samt med den dataansvarliges instrukser. Der er behov for mere klarhed på dette punkt. Derfor foreslår WP29 at tilsikre, at tilstrækkelighedsafgørelsen fremsætter flere oplysninger, for eksempel ved at indsætte en klar henvisning til princippet om formålsbegrænsning (bilag II, II.5), og i henhold hertil må data ikke behandles (inklusive offentliggøres) til uforenelige formål inden for princippet om videregivelse (foruden frameldingsprincippet).

[20] Behovet for bindende og retsgyldige forpligtelser er også fremhævet i GDPR uanset det anvendte værktøj (BCR'er, kontraktbestemmelser, adfærdskodekser eller certificering).
[21] For eksempel for HR-data.

Behov flere forpligtelser for organisationer under værnet om privatlivets fred, der fungerer som en behandler (agent), og som sender data videre til en anden behandler (agent)

Manglen på klare regler, hvor værnorganisationen fungerer som en agent (dvs. på vegne af en dataansvarlig i EU), indikerer et smuthul og kan eventuelt forhindre den dataansvarlige i EU i at bevare ledelsen. En værnorganisation, der modtager data som en agent for en dataansvarlig i EU, skal respektere den dataansvarlige i EU's instrukser. Dette skal være udtrykkeligt fremsat i principperne for at sikre, at manglende respekt for disse instrukser ikke kun vil føre til et kontraktbrud (bilag II, III.10.a.ii), men også til en overtrædelse af principperne for værnet om privatlivets fred.

Muligheden for, at en værnorganisation, der fungerer som agent, senere videregiver data til en tredjepartsagent, skal gøres gennemskuelig for den dataansvarlige og afhænge af dennes forudgående godkendelse. Derfor skal det klart fremsættes, at det er kontrakten, underskrevet af agenten med den dataansvarlige i EU (henvist til i Ofte stillede spørgsmål 10 som "Artikel 17 kontrakt"), der skal afgøre, om en videregivelse er tilladt[22].

De aktuelle betingelser, der gælder for videregivelsen til en agent, bygger på antagelsen, at værnorganisationen fungerer som en dataansvarlig og derfor selv kan bestemme den mulige indblanding fra en tredjepartsagent. Dette bør imidlertid ikke være muligt, hvor værnorganisationen fungerer som en agent. Ellers bliver den dataansvarlige i EU frataget sine kontrolkapaciteter.

De relevante bestemmelser for privatlivets fred i kontrakten, der er afsluttet med tredjepartsagenten, skal gøres tilgængelige for den dataansvarlige og skal også yde mindst samme beskyttelsesniveau, som kontrakten underskrevet med den dataansvarlige yder.

2.2.4 Dataintegritet og formålsbegrænsning

a) Proportionalitet

I forbindelse med en mindre detalje henviser WP29 til sit brev til næstformand Viviane Reding, hvori der skrives, at "en behandling af persondata ikke kan, selv under streng respekt for meddelelse og valg, være proportional, hvad angår interessernes rettigheder og friheder for registrerede eller samfundet. Princippet om proportionalitet eller rationalitet skal respekteres i alle behandlingsfaserne og skal endvidere være gældende for principperne for meddelelse og valg"[23].

Værnet om privatlivets fred (bilag II, II.5.a) fremsætter, at oplysningerne skal være begrænset til det, der er relevant for behandlingen. WP29 vil foretrække, hvis formuleringen ændres i den endelige tilstrækkelighedsafgørelse, da det faktum, at dataene skal være relevante for behandlingen, ikke er tilstrækkeligt til at gøre behandlingen proportional. For at imødekomme

[22] Se WP29's brev til næstformand Viviane Reding dateret 10. april 2014, punkt 4 under Videregivelse.
[23] Se WP29's brev til næstformand Viviane Reding dateret 10. april 2014, punkt 8.

proportionalitetsprincippet skal behandlingen være begrænset til de data, der er nødvendige for den behandling, der er på spil.

b) Nøjagtighed

Princippet om dataintegritet og formålsbegrænsning (bilag II, II.5) fremsætter også: "En organisation skal i det omfang, det er nødvendigt, træffe passende foranstaltninger for at sikre, at persondata er pålidelige, nøjagtige, fuldstændige og ajourførte". WP29 anfører, at dette er præcist den samme formulering, som blev anvendt i Safe Harbour-ordningen. WP29 tvivler på, at formuleringen "i det omfang, der er nødvendigt for disse formål" skal inkluderes, da nøjagtigheden af dataene efter dens mening ikke skal afhænge af behandlingsformålet. WP29 vil foretrække, hvis denne forbindelse ikke skabes i den endelige tilstrækkelighedsafgørelse.

c) Formålsbegrænsning

Hvor persondata videregives til en amerikansk organisation af en dataansvarlig, der er veletableret i EU, skal dataeksportøren udtrykkeligt informere den amerikanske organisation om formålene, hvortil dataene oprindeligt blev indsamlet. Dette er afgørende for at fastslå, om en formålsændring finder sted efter videregivelsen, hvormed princippet om meddelelse og valg udløses, og vil bidrage til allokeringen af risiko og ansvar.

Princippet om dataintegritet og formålsbegrænsning (bilag II, II.5) fremsætter, at en organisation ikke må behandle personlige oplysninger på en måde, der er uforenelig med de formål, hvortil de er blevet indsamlet eller efterfølgende autoriseret af den fysiske person. Valgprincippet (bilag II, II.2) tilvejebringer imidlertid en tilmelding til "brugen" af følsomme oplysninger (dvs. personlige oplysninger, der præciserer medicinske eller sundhedstilstande, racemæssig eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab eller oplysninger, der præciserer den fysiske persons sexliv, samt data vedrørende straffeattester) til formål, som afviger væsentligt fra de formål, hvortil dataene oprindeligt blev indsamlet eller efterfølgende autoriseret af den fysiske person. Denne tilmelding er ikke påkrævet i de situationer, der er nævnt i tillægsprincippet 1.a (bilag II, III.1.a). Hvad angår ikke-følsomme personlige oplysninger, er der sørget for et frameldingssystem.

WP29 anfører, at anvendelsesområdet for princippet om formålsbegrænsning er anderledes under principperne for meddelelse, valg samt dataintegritet og formålsbegrænsning. Faktisk bruges begreberne "uforeneligt formål" og "væsentligt afvigende formål" i den samme tekst uden en klar definition af begge disse begreber[24].

WP29 har alvorlige bekymringer vedrørende det faktum, at sådan inkonsistens kan føre til store problemer med at afstemme princippet om dataintegritet og formålsbegrænsning (bilag II, II.5) med valgprincippet (bilag II, II.2), da den ene anfører, at dataene ikke kan behandles på en måde, der er uforenelig med de formål, hvortil de blev indsamlet, mens den anden

[24] WP29 anførte, at der også bruges nogle andre begreber: "En brug, der ikke er konsekvent med" (bilag II, III.14.b.ii), en "brug til andre formål" (bilag II, III. 9.B.i), en "brug til et andet formål end det, hvortil de oprindeligt blev indsamlet" (bilag II, II.1.b). Denne uklarhed kan føre til manglen på tilstrækkelige garantier, hvad angår princippet om formålsbegrænsning.

tilvejebringer en frameldingsmekanisme i tilfælde af, at dataene bliver behandlet til et formål, der afviger væsentligt fra det originale formål.

Dermed kan valgprincippet læses som en autorisation af en yderligere uforenelig behandling[25]. Ifølge WP29 har den gjort det klart, at en organisation ikke skal være autoriseret til at behandle data til et formål, der er væsentligt afvigende, hvor formålet er uforeneligt i henhold til princippet om formålsbegrænsning. Med andre ord skal det stå klart, at valgprincippet ikke er en undtagelse af formålsbegrænsningen.

Hvis den yderligere behandling kan anses som værende forenelig, så skal meddelelses- og valgprincipperne under alle omstændigheder også være gældende.

2.2.5 Journalistiske undtagelser

De journalistiske undtagelser fra behandlingen af persondata er dækket i tillægsprincip 2 (bilag II, III.2). Det er underforstået, at disse bestemmelser afspejler den amerikanske forfatningsretlige beskyttelse af ytringsfrihed. Derfor anfører dokumenterne til værnet om privatlivets fred, at "personlige oplysninger, der findes i tidligere publiceret materiale udbredt fra mediearkiver, ikke er underlagt kravene i principperne om værnet om privatlivets fred" (bilag II, III.2.b). Denne undtagelse lader til at inkludere al yderligere behandling af en dataansvarlig eller -behandler, dvs. skal ikke begrænses til yderligere behandling til journalistiske formål. Som allerede anført i brevet til næstformand Viviane Reding dateret 10. april 2014 ville WP29 have foretrukket at se en mere begrænset fremgangsmetode for journalistiske undtagelser, mere på linje med princippet som anvendt i EU, samt retten til at fjerne ting fra lister efter sagen med Google Spain[26].

2.2.5 Ret til aktindsigt, rettelse og sletning for registrerede

I henhold til værnet om privatlivets fred har fysiske personer ret til at få *bekræftelse* på, om deres data bliver behandlet af organisationen, og til at få sådanne data *meddelt* (bilag II, III.8.a.i). Organisationers forpligtelse til at svare på anmodninger fra fysiske personer vedrørende behandlingsformålene, kategorierne for de pågældende persondata og modtagerne eller modtagerkategorierne, hvortil de persondata offentliggøres, er imidlertid ret svag. WP29 mener, at de oplysninger, der skal udleveres til registrerede, skal nævnes i tekstens hoveddel, fremfor blot i en fodnote, og der skal laves udkast til dem som en klar forpligtelse (forbundet med bilag II, III.8.a.i.1).

Ifølge tillægsprincip 8 "skal aktindsigt kun stilles til rådighed i det omfang, at en organisation opbevarer de personlige oplysninger" (bilag II, III.8.d.ii). Denne regel skal ikke tolkes restriktivt, i den forstand at aktindsigt, i princippet, skal stilles til rådighed for data, der behandles af en organisation og ikke bare opbevares. Til formål for effektiv aktindsigt er det derfor vigtigt at gøre det klart, at "opbevarer" betyder "behandler" i den definitions betydning,

[25] Se også bemærkningen under valgprincippet. WP29 mener, at det faktum, at reglerne for videregivelse (bilag II, II.3) kun henviser til valgprincippet og ikke til princippet om formålsbegrænsning, øger risikoen for en sådan forståelse.
[26] Sag C-131/12 – Google Spain mod Agencia Española de Protección de Datos og Mario Costeja González, 13. maj 2014.

som er fremsat i bilag II, I.8.b. Anvendelsen af denne regel skal undersøges nøje under den fælles evaluering af værnet om privatlivets fred.

Der er fortsat bekymringer, hvad angår listen med undtagelser, som er fremsat i bilag II, III.8.e.(i), og som er tilsvarende den, der er fremsat af Ofte stillede spørgsmål 8 i Safe Harbour, og som har en tendens til at hælde mod organisationernes interesser. I denne forstand vil indsigt i deres egne persondata ikke blive bevilliget til fysiske personer af følgende årsager: "brud på et professionelt privilegium eller forpligtelse" (bilag II, III.8.e.3), "præjudicering af undersøgelser af medarbejdersikkerhed eller klageprocedurer eller i forbindelse med afløserplanlægning for medarbejdere og virksomhedsreorganisering" (bilag II, III.8.e.4) og "præjudicering af den fortrolighed, der er nødvendig til overvågnings-, inspektions- eller regulatoriske funktioner forbundet med lovlig ledelse eller i fremtidige eller igangværende forhandlinger, der involverer organisationen" (bilag II, III.8.e.5). Disse årsager skal læses i tillæg til den generelle undtagelse fra fortrolige, kommercielle oplysninger, som er inkluderet i bilag II, III.8.c. Derfor vil en fysisk person aldrig have aktindsigt i de situationer nævnt ovenfor, ingen ligevægt mellem den fysiske persons rettigheder og interesser og organisationens rettigheder og interesser, som skal nå en løsning på indsigtsanmodningen.

WP29 minder om, at retten til at tilgå deres egne data bliver bevilliget til fysiske personer i artikel 8, stk. 2, i charteret. Mens dette ikke er en absolut ret, er den principiel for retten til beskyttelse af persondata, da den gør det muligt at udøve den registreredes andre rettigheder, såsom rettelse og sletning.

Hvad angår retten til rettelse og sletning bifalder WP29 en væsentlig forbedring, som principperne om værnet for privatlivets fred har bragt med sig, sammenlignet med principperne om Safe Harbor, forudsat at disse rettigheder ikke kun bliver bevilliget i situationer, hvor data er unøjagtige, men også hvor data er blevet behandlet i overtrædelse af principperne (bilag II, II.6).

2.2.6 Regres, håndhævelse og ansvar (afhjælpningsmekanismer)

a) Effektiv udøvelse af fysiske personer i EU's afhjælpningsrettigheder

WP29 anerkender de amerikanske myndigheders forpligtelser i forbindelse med afhjælpningsmekanismens forskellige lag. I betragtning af kompleksiteten ved og manglen på klarhed i mekanismens samlede opbygning frygter WP29, at den effektive udøvelse af den registreredes rettigheder i praksis kan være undermineret. WP29 påpeger, at afhjælpningsmekanismens kvalitet skal råde over den mængde mekanismer, der er tilgængelige for fysiske personer i EU. Der er også bekymringer om, at de fleste, hvis ikke alle, regresmekanismer forudser en procedure i USA, hvormed europæiske databeskyttelsesmyndigheders overvågning af proceduren vanskeliggøres.

Faktisk fokuserer regresmekanismen, der fremsættes i værnet om privatlivets fred, først på muligheden for, at den registrerede "opretholder sine rettigheder og forfølger sagen med

manglende overholdelse af principperne om privatlivets fred gennem direkte kontakter med den amerikanske, selvcertificerede virksomhed"[27]. Organisationer skal endvidere udpege en uafhængig stridsløsningsinstans, som skal undersøge og løse individuelle klager. WP29 bifalder det faktum, at den vil være organiseret uden nogen omkostninger for den fysiske person.

Alternativt kan klager indgives direkte til Federal Trade Commission, selv hvis FTC ikke har nogen pligt til at behandle dem. En databeskyttelsesmyndighed kan også henvise en klage, og det amerikanske handelsministerium har forpligtet sig til at evaluere og gøre sit bedste for at fremme en løsning på klager (bilag I), som vil blive givet "prioritet" af Federal Trade Commission (bilag II, III.7.e). FTC's prioritering af klager fremsætter imidlertid ingen sikkerhed for den registrerede om, at dennes klage vil blive behandlet.

Som en sidste udvej vil fysiske personer have mulighed for at påberåbe sig bindende voldgift. Voldgiftspanelet vil være hjemmehørende i USA og være underlagt evalueringer af de amerikanske domstole.

Værnet om privatlivets fred giver også organisationen mulighed for at vælge at samarbejde med databeskyttelsesmyndigheder i EU (bilag II, III.5.a). Det er endda obligatorisk for HR-data, der er indsamlet i konteksten af et ansættelsesforhold (bilag II, III.9.d.ii). I et sådant scenarie vil alternativ stridsløsning ikke være gældende (bilag II, III.5.a). Værnet om privatlivets fred fastsætter ikke klart, hvordan samarbejdet med databeskyttelsesmyndigheder i EU vil blive organiseret i praksis. Det er især uklart, om panelet vil behandle alle sager, eller om hver forskellig sag vil blive behandlet af et andet panel.

WP29 mener, at flere oplysninger er påkrævet i tilstrækkelighedsafgørelsen, hvad angår databeskyttelsesmyndigheders kompetence til at behandle klager. Dette afhænger tilsyneladende af organisationens kvalifikation, men det er uklart hvordan.

Hvor organisationen fungerer som en agent på vegne af en dataansvarlig i EU, vil fysiske personer under alle omstændigheder have mulighed for at klage til den kompetente databeskyttelsesmyndighed i EU. Denne situation vil være ens for både HR og anden kommerciel databehandling.

Hvor organisationen under værnet om privatlivets fred fungerer som en dataansvarlig, vil en databeskyttelsesmyndigheds kompetence til at behandle klagen være begrænset til behandling underlagt EU-lovgivning (behandling under ansvar af den dataansvarlige i EU) – inklusive fælles kontrol med den amerikanske organisation – eller hvor organisationen under værnet om privatlivets fred vil være direkte underlagt EU-lovgivning, for eksempel ved at bruge udstyr i EU). For databehandling, der kun foretages under amerikansk lov, vil mekanismerne til værnet om privatlivets fred imidlertid gælde eksklusivt. For at overvinde sprogbarrierer og mangel på kendskab til det amerikanske retssystem kan det være en hjælp, hvis databeskyttelsesmyndigheder i EU er berettigede til at fungere som en mægler for den fysiske persons klage eller til at hjælpe ham/hende i procedurer med alternative stridsløsninger med

[27] Europa-Kommissionen, udkast til tilstrækkelighedsafgørelse, § 30.

amerikanske organisationer eller under deres kontakt med de amerikanske myndigheder, hvis databeskyttelsesmyndigheden anser det for passende.

WP29 understreger, at mekanismen, der er forklaret i værnet om privatlivets fred, ikke følger de tidligere anbefalinger, ud fra hvilke fysiske personer i EU skal være "i stand til at fremsætte erstatningskrav i Den Europæiske Union" samt "bevilliges retten til at indgive et erstatningskrav for en kompetent national domstol i EU"[28]. Der vil sættes pris på, hvis organisationer under værnet om privatlivets fred ville inkludere en sådan mulighed i deres politikker om privatlivets fred.

For at sikre effektivitet anbefaler WP29, at systemet fortrinsvist skal tillade databeskyttelsesmyndigheder i EU at repræsentere den registrerede og handle på dennes vegne eller at fungere som en mægler. Alternativt skal den indeholde specifikke jurisdiktionsbestemmelser, der giver registrerede ret til at udøve deres rettigheder i Europa.

b) Voldgift

Endelige voldgiftsprocedurer er endnu ikke gjort færdige, hvilket vanskeliggør WP29's vurdering. Da det lader til, at voldgiftsordningen vil finde sted under amerikansk lov, og at procedurens eneste sprog vil være engelsk, vil databeskyttelsesmyndigheder i EU eventuelt ønske at have ret til at hjælpe fysiske personer i processen.

Desuden er voldgiftsproceduren blevet iværksat som følge af det faktum, at der ikke var nogen forsikring om, at en klage ville blive behandlet, da FTC ikke har pligt til at behandle alle klager. Hvis en fysisk person i EU føler behov for hjælp fra en advokat, anfører WP29, at vedkommende vil skulle dække sin egen advokats salær, hvilket kan forhindre fysiske personer i at indsende deres klage til voldgiftsproceduren.

c) Afhjælpningsmekanismernes tilsyn, håndhævelse og effektivitet

<u>Betingelser for at komme ind i værnet</u>

Ifølge EU-Domstolen "er et selvcertificeringssystems pålidelighed […] praktisk talt baseret på etableringen af effektive registrerings- og opsynsmekanismer, der muliggør overtrædelser af reglerne, hvilket sikrer beskyttelsen af de grundlæggende rettigheder […]"[29].

WP29 anfører, at det amerikanske handelsministeriums rolle under værnet om privatlivets fred i certificeringsprocessen lader til at være reduceret til blot at tjekke dokumenters fuldstændighed. Selvom WP29 anerkender, at selvcertificering ikke forudsætter en systematisk a priori kontrol af implementeringen af politikkerne om privatlivets fred, skal det amerikanske handelsministerium som et absolut minimum forpligte sig til systematisk at kontrollere, at politikkerne om privatlivets fred omfatter alle principperne om værnet om

[28] Se WP29's brev til næstformand Viviane Reding dateret 10. april 2014.
[29] EU-Domstolen, Schrems, § 81.

privatlivets fred. Sådanne forpligtelser er nævnt i udkastet til tilstrækkelighedsafgørelsen, men kan ikke klart identificeres i det amerikanske handelsministeriums repræsentationsbrev[30].

Et brud på principperne om værnet om privatlivets fred kan gå ubemærket hen i længere tid og vil muligvis kun blive registreret, efter den registreredes grundlæggende rettigheder har lidt alvorlig skade, muligvis uoprettelig skade. Således kan denne fremgangsmetode være i strid med det europæiske sikkerhedsprincip.

Gennemsigtighed ved hjælp af listen for værnet om privatlivets fred og fortegnelse over organisationer, der er fjernet fra listen

Der er foretaget væsentlige forbedringer, hvad angår gennemsigtigheden for den registrerede. Foruden alle amerikanske organisationer, der har selvcertificeret sig over for det amerikanske handelsministerium, vil den nye liste for værnet om privatlivets fred også indeholde en fortegnelse over alle organisationer, der er fjernet fra listen for værnet om privatlivets fred, inklusive årsagen til, at organisationen blev fjernet[31]. Det amerikanske handelsministeriums websted for værnet om privatlivets fred fokuserer mere på målgrupper på en måde, der vil fremme verificeringen af den type oplysninger, der er dækket af en organisations selvcertificering samt politikken om privatlivets fred, der gælder for de dækkede oplysninger, og metoden, som organisationen bruger til at verificere dens overholdelse af principperne[32]. WP29 bifalder det faktum, at det nu er tydeligt, at det amerikanske handelsministerium vil kontrollere, om virksomheder, der har offentlige websteder, offentliggør deres politik om privatlivets fred på dette websted, eller, når de ikke har noget offentligt websted, hvor politikken om privatlivets fred er gjort tilgængelig for offentligheden[33]. Dokumenterne er også mere informative om indholdet i politikken om privatlivets fred[34].

WP29 mener, at der kan opstå et problem, hvis en organisation, som allerede er inkluderet på listen for værnet om privatlivets fred, efterfølgende udvider dens certificering til andre datakategorier. I sådanne tilfælde vil listen ikke afspejle de forskellige perioder for princippernes anvendelighed af de forskellige datakategorier. Dette skaber risikoen for, at fysiske personer og forretninger i EU ikke helt kan vurdere, om et bestemt datasæt rent faktisk er underlagt principperne om værnet om privatlivets fred, og hvis det er tilfældet, siden hvornår. For at undgå denne utilstrækkelighed anbefaler arbejdsgruppen, at en organisations fortegnelse på listen for værnet om privatlivets fred skal angive ikrafttrædelsesdatoen for selvcertificeringen separat for hver kategori af persondata.

WP29 bifalder det faktum, at det amerikanske handelsministerium vil opretholde en fortegnelse over organisationer, der er blevet fjernet fra listen for værnet om privatlivets fred,

[30] Europa-Kommissionen, udkast til tilstrækkelighedsafgørelse, § 34.
[31] Bilag I, punkt 5 og bilag II, II.1; WP29 henviser også til den fjerde af Kommissionens anbefalinger, som blev fremsat i meddelelsen COM(2103)847 samt WP29's brev til næstformand Viviane Reding dateret 10. april 2014, især punkt 5 under "Gennemsigtighed".
[32] Bilag I, punkt 8; WP29 henviser også til sit brev til næstformand Viviane Reding dateret 10. april 2014, især punkt 2 under "Gennemsigtighed".
[33] Bilag I, punkt 3 og 4; WP29 henviser også til den første af Kommissionens anbefalinger, som blev fremsat i meddelelsen COM(2103)847 samt WP29's brev til næstformand Viviane Reding dateret 10. april 2014, især punkt 3 under "Gennemsigtighed".
[34] Bilag I, punkt 5 og 6 samt bilag II, III.6.

og at denne fortegnelse vil inkludere en forklaring, der afklarer, at disse organisationer ikke længere er sikret fordelene ved værnet om privatlivets fred, men fortsat skal anvende principperne til persondata, der modtages, mens den er en certificeret organisation under værnet om privatlivets fred, så længe de opbevarer sådanne data (bilag I, punkt 3). Da nogle organisationer, som er blevet fjernet fra listen for værnet om privatlivets fred, kan vælge at returnere eller slette de data, der er modtaget under værnet om privatlivets fred, mens andre organisationer vil opbevare data, de har modtaget under værnet, er det imidlertid vigtigt at give fysiske personer mere gennemsigtighed på dette område. Derfor skal fortegnelsen over virksomheder, der opretholdes af det amerikanske handelsministerium, angive, om organisationen stadig opbevarer persondata, der er modtaget under værnet om privatlivets fred, eller om den har returneret eller slettet sådanne data. Hvis organisationen stadig opbevarer sådanne data, skal fortegnelsen udtrykkeligt anføre, at organisationen fortsat skal anvende principperne til sådanne data.

Fortegnelsen, der opretholdes af det amerikanske handelsministerium, skal endvidere nævne, at disse organisationer ikke længere er sikret fordelene ved værnet om privatlivets fred for nye videregivelser, hvilket betyder, at organisationen ikke længere har tilladelse til at modtage persondata fra EU under principperne.

Verifikationsprocedurer

For at verificere, at selvcertificeringen er effektiv i praksis, kan organisationer foretage selvvurderinger eller eksterne overholdelsesevalueringer. WP29 beklager, at medarbejderes undervisning kun er påkrævet, når en organisation opterer for verificering via selvvurderinger (bilag II, III.7.c). Det lader også til, at behovet for at kontrollere, at politikkerne er nøjagtige, omfattende, prominent fremsat, implementeret og tilgængelige, kun er påkrævet, hvis organisationen opterer for intern evaluering (selvvurdering), og at evaluering af en ekstern mekanisme kun er begrænset til overholdelse af organisationens politik om privatlivets fred.

A posteriori

WP29 bifalder, at FTC og det amerikanske handelsministerium er tildelt undersøgelsesbeføjelser i klagesager. WP29 anfører desuden, at det amerikanske handelsministerium vil have mulighed for at foretage ex officio verificeringer, især via afsendelse af spørgeskemaer. WP29 ønsker imidlertid at sikre, at en sådan fremgangsmetode er tilstrækkelig til at opfylde EU-Domstolens krav om effektive registrerings- og tilsynsmekanismer for brud. Faktisk har WP29 stadig spørgsmål til amerikanske håndhævelsesmyndigheders præcise beføjelser til at udføre inspektioner på stedet hos selvcertificerede organisationer til at undersøge brud på værnet om privatlivets fred, til hvordan *eksekvatur* af en EU-myndigheds beslutning kan opnås på det amerikanske område, og til hvordan sanktionerne under værnet om privatlivets fred er præventivt i praksis.

2.2.7 Behandling af HR-data

Anvendelsesområde

Tillægsprincip 9 (bilag II, III.9) gælder for personlige oplysninger om en medarbejder (tidligere eller nuværende), som er indsamlet i konteksten af ansættelsesforholdet. I henhold til formuleringen af tillægsprincip 9.a.ii gælder principperne om værnet om privatlivets fred udelukkende, når "identificerede fortegnelser videregives eller tilgås". Begrebet "identificeret fortegnelse" er ikke på linje med definitionen af "persondata" under bilag II, I.8.a., som består af "data om en identificeret eller identificerbar fysisk person", og kan derfor ikke afstemmes med definitionen, der bruges i direktivet[35].

Tillægsprincip 9.a.ii anfører, at "statistisk rapportering, der er afhængig af samlede ansættelsesdata, og som ikke indeholder nogen persondata eller brugen af anonymiserede data giver ikke anledning til bekymring i forbindelse med privatlivets fred". Dette udsagn er i modstrid med flere konklusioner, der er fremsat af WP29. WP29 ønsker også at understrege, at samlede data stadig kan genidentificeres og derfor skal anses som persondata[36].

[35] Som allerede understreget er begrænsningen for fortegnelser, der "videregives eller tilgås" heller ikke på linje med begrebet "behandling" (bilag II, I.8.b).
[36] Se konklusion 4/2007 vedrørende begrebet med persondata samt konklusion 05/2014 vedrørende anonymiseringsteknikker.

Meddelelse, valg og formålsbegrænsning

Tillægsprincip 9.b.i kommer med et eksempel på anvendelse af meddelelses- og valgprincipperne, hvor der anvendes HR-data til et andet formål. Eksemplet vedrører en amerikansk organisation, som "har til hensigt at anvende personlige oplysninger, der er indsamlet gennem ansættelsesforholdet til formål, der ikke er ansættelsesrelaterede, såsom markedsføringsmeddelelser. I dette scenarie er ændringen af formålet autoriseret under betingelsen om at respektere meddelelses- og valgprincippet. I henhold til WP29 vil yderligere behandling af HR-data til direkte markedsføringsformål i de fleste tilfælde skulle anses som et uforeneligt formål og dermed i modstrid med princippet om formålsbegrænsning (bilag II, II.5.a). WP29 mener endvidere, at valget ikke kan være et passende grundlag for medarbejderens "samtykke" (framelding) til en ændring af formålet, i ansættelseskonteksten, hvor sådant samtykke eventuelt ikke er helt gratis.

WP29 har store betænkeligheder ved, at det primære fokus, som værnet om privatlivets fred lægger på valgprincippet som en betingelse for yderligere brug af data til et andet formål, imødekommer OECD's retningslinjer for privatlivets fred, da der ikke er nogen tilstrækkelige garantier for at forhindre, at denne frameldingsmekanisme også kan bruges til yderligere behandling til uforenelige formål. Tillægsprincip 9.b.iv sørger for en bred og udtrykkelig undtagelse fra meddelelses- og valgprincipperne "i det omfang og i den periode, som er nødvendig for at undgå præjudicering af organisationens evne til at tage beslutninger om forfremmelser, udnævnelser eller andre lignende ansættelsesbeslutninger. Først skal brugen af HR-data til sådanne formål allerede være udtrykkeligt fremsat ved indsamlingen af dataene. Desuden er formuleringen "andre lignende ansættelsesbeslutninger" for vag og for bred. Konsekvensen vil være, at HR-data helt er undtaget fra meddelelses- og valgprincippet, hvor de behandles i konteksten af ansættelsesforhold. Begrebet er så bredt, at det ikke gør det muligt at vurdere, om den yderligere brug er forenelig med det originale formål. WP29 anbefaler, at denne undtagelse slettes.

Aktindsigt

Tillægsprincip 9.e.i sørger også for en undtagelse, der skal gælde for adgangsprincippet eller fra at indgå kontrakt med en tredjeparts dataansvarlige for HR-data, hvor de vedrører sporadiske ansættelsesrelaterede aktiviteter, såsom reservation af fly, hotelværelse eller forsikringsdækning, videregivelser af persondata fra et lille antal medarbejdere, og forudsat at meddelelses- og valgprincipperne er overholdt. WP29 ser ingen rimelig begrundelse for en sådan undtagelse og anbefaler, at dette afsnit slettes.

2.2.8 Farmaceutiske produkter og medicinsk udstyr

Anvendelsesområde

Værnet om privatlivets fred anser ikke videregivelser af nøglekodede data fra Den Europæiske Union til USA i forbindelse med farmaceutiske produkter og medicinsk udstyr for at udgøre videregivelser, der vil være omfattet af værnet om privatlivets fred (Bilag II,

III.14.g.i). Videregivelsen af nøglekodede data nyder imidlertid godt af beskyttelse under europæiske databeskyttelseslove. Det betyder, at værnet om privatlivets fred i praksis ikke kan dække sådanne videregivelser. WP29 opfordrer Europa-Kommissionen til udtrykkeligt at fremsætte, at udkastet til tilstrækkelighedsafgørelsen ikke vil dække videregivelsen af nøglekodede data af farmaceutiske eller medicinske årsager, og sådanne videregivelser skal derfor være dækket af andre sikkerhedsforanstaltninger, såsom Standardkontraktbestemmelser (i det følgende benævnt: SCC'er) eller BCR'er. WP29 indikerer, at dette kunne præciseres i den endelige tilstrækkelighedsafgørelse.

Overførsler til regulatoriske og tilsynsformål (bilag II, III.14.d)

WP29 er bekymret for, at det under disse bestemmelser er muligt at overføre personoplysninger, som på grund af deres medicinske karakter overvejende er følsomme oplysninger, til amerikanske myndigheder. Da værnet om privatlivets fred er designet til dataoverførsler mellem private enheder, må det derfor antages, at et offentligt organ som for eksempel en amerikansk myndighed, ikke er omfattet af kravet om selvcertificering ifølge værnet om privatlivets fred, hvilket derfor rejser spørgsmålet om passende databeskyttelse i forbindelse med sådanne overførsler. Hvis sådanne videregivelser skal administreres til regulatoriske formål, skal der tages passende sikkerhedsforanstaltninger til at sikre vedvarende beskyttelse af den EU-registreredes grundlæggende rettigheder. WP29 understreger det faktum, at udkastet til tilstrækkelighedsafgørelsen ikke fremsætter nogen konklusioner desangående. Derfor har WP29 ikke nogen garantier for, at EU-registreredes følsomme data vil have tilstrækkelig beskyttelse i denne kontekst.

Endvidere anfører WP29, at den ikke forstår, hvorfor formålet med "markedsføring" er anført som et eksempel på behandling til fremtidig videnskabelig forskning. Desuden er årsagen til at give videregivelser til virksomhedssteder og andre forskere (bilag II, III.14.d) under overskriften "Videregivelser til regulatoriske og tilsynsformål" uklar. Disse problemer behøver afklaring i den endelige tilstrækkelighedsafgørelse.

Produktsikkerhed, overvågning af virkekraft (inklusive rapportering til statslige organer) og sporing af patienter ved hjælp bestemte lægemidler eller bestemt medicinsk udstyr

Værnet om privatlivets fred fremsætter en undtagelse fra principperne om meddelelse, valg, videregivelser og aktindsigt i det omfang, at overholdelse af princippet interfererer med overholdelse af regulatoriske krav. Udkastet til tilstrækkelighedsafgørelsen fremsætter ikke nogen konklusioner, hvad angår situationen, hvor principperne om privatlivets fred interfererer med overholdelsen af regulatoriske krav. Hvis WP29 eventuelt kunne forstå, at statsundersøgelser kan berettige grænser for meddelelser og aktindsigt for at beskytte undersøgelser, ser WP29 ikke årsagerne, der kan berettige sådanne brede undtagelser, hvor behandling foretages af organisationen eller af en tredjepart inden for den private sektor. Da for eksempel patientbehandlinger bliver stadig mere skræddersyede, er en sådan omfattende undtagelse fra principperne i værnet om privatlivets fred i forbindelse med sporing af patienter, som behandles med visse lægemidler eller medicinsk udstyr, uacceptabel, da denne behandlingsform vil vinde stadig mere frem. Dette gælder også, hvor dataene anvendes af

medicinalvirksomheder til produktsikkerhed, overvågning af virkegrad (test eller salg af nye lægemidler).

2.2.9 Offentligt tilgængelige oplysninger

Undtagelsen til aktindsigt i tilfælde af offentligt tilgængelige oplysninger og offentlige fortegnelsesoplysninger (bilag II, III.15.d and e) giver anledning til bekymring om det omfang, en fysisk person, når vedkommende benytter sin aktindsigt, er interesseret i at vide, om en bestemt dataansvarlig behandler data om ham/hende, samt at vide, hvilke data der bliver behandlet for at være i stand til at kontrollere behandlingen af hans/hendes data. WP29 har gentagne gange fremsat, at registrerede i henhold til EU-lovgivningen altid har ret til at tilgå deres data og, hvor det er nødvendigt, kræve rettelse eller sletning af dataene, hvis dataene ikke er blevet behandlet på lovlig vis, eller hvis de er ufuldstændige eller unøjagtige, uanset om de persondata er blevet publiceret eller ej[37]. Hvis den fysiske persons indsigtsanmodning bliver afvist på det grundlag, at dataene blev skaffet fra offentligt tilgængelige kilder eller offentlige fortegnelser, vil den fysiske person miste muligheden for at styre dataenes nøjagtighed og til at styre, om dataene blev gjort offentlige på lovlig vis i første omgang.

Værnet om privatlivets fred undtager imidlertid offentlige fortegnelser og offentligt tilgængelige oplysninger fra principperne om meddelelse, valg, aktindsigt og ansvarlighed for videregivelser (bilag II, II.15.b). Disse undtagelser forekommer for brede sammenlignet med direktivet og giver anledning til bekymring, da de blandt andet hæmmer de fysiske personers muligheder for at styre nøjagtigheden af deres data og for at begrænse udbredelsen af deres data.

2.3 Konklusioner

WP29 anerkender, at de amerikanske myndigheder og Europa-Kommissionen i væsentlig grad har forbedret de kommercielle aspekter ved dataoverførsler mellem de to kontinenter. Når der tages højde for ovennævnte analyse, mener WP29 dog, at den kommercielle del ved værnet om privatlivets fred behøver yderligere afklaring på mange punkter. For eksempel vækker manglen på et udtrykkeligt princip om dataopbevaring grund til bekymring. Derfor har WP29 alvorlige bekymringer om, at værnet om privatlivets fred kan sikre et beskyttelsesniveau, der i bund og grund svarer til det i EU.

Tilstrækkelighedsafgørelsen skal yderligere afklare principperne om formålsbegrænsning og valg. Der er fortsat risici for smuthuller i forbindelse med flere principper, især videregivelserne, klagehåndteringsmekanismen og behandlingen af HR-data og farmaceutiske data. Hvordan principperne om privatlivets fred skal gøres gældende for databehandlere (agenter), kræver desuden yderligere uddybning, og særlig opmærksomhed er nødvendig for at sikre en klar og utvetydig anvendelse af terminologi.

[37] Se WP20, punkt 4.

3. VURDERING AF GARANTIERNE FOR NATIONAL SIKKERHED I UDKASTET TIL TILSTRÆKKELIGHEDSAFGØRELSEN

3.1 Sikkerhedsforanstaltninger og begrænsninger, der er relevante for amerikanske myndigheder for national sikkerhed

Indgreb i grundlæggende rettigheder for privatlivets fred og databeskyttelse kan eventuelt tillades, forudsat at sådant indgreb kan forsvares i et demokratisk samfund. Det betyder, at principperne om privatlivets fred ikke er endelige, og at undtagelsesbestemmelser kan være mulige, men kun hvis de relevante (afgørende) garantier er opfyldt. I overensstemmelse med målet om øget beskyttelse af privatlivets fred skal organisationer desuden tilstræbe at implementere principperne på en fuldstændig og gennemsigtig måde, inklusive en angivelse i deres politikker om privatlivets fred, hvor undtagelser af principperne, der er tilladt af det amerikanske retsvæsen, vil være gældende regelmæssigt. Når principperne og/eller den amerikanske lovgivning giver mulighed derfor, forventes organisationerne af samme årsag at vælge et højere beskyttelsesniveau.

I bilag II, I.5 fremsættes det, at "overholdelse af principperne om privatlivets fred kan være begrænset: a) til et niveau, der er tilstrækkeligt for at opfylde kravene med hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden, b) af love, administrative bestemmelser eller retspraksis, der medfører modstridende forpligtelser eller udtrykkelige tilladelser, såfremt foretagender i forbindelse med anvendelsen af sådanne tilladelser kan påvise, at de kun overtræder principperne i det omfang, som er nødvendigt for at tilgodese de altovervejende legitime interesser, som den pågældende tilladelse har til hensigt at fremme, eller c) i det omfang, direktivet eller medlemsstaternes lovgivning tillader undtagelser eller dispensationer, såfremt sådanne undtagelser eller dispensationer også finder anvendelse i sammenlignelig kontekst.

Spørgsmålet er, om undtagelsesbestemmelserne nævnt i bilag II kan forsvares i et demokratisk samfund. I henhold til udkastet til afgørelsen om tilstrækkeligheden af værnet om privatlivets fred, har Kommissionen konkluderet, "at USA har indført regler, hvorved det tilsigtes at begrænse de eventuelle indgreb af hensyn til den nationale sikkerhed i de grundlæggende rettigheder hos de personer, hvis oplysninger overføres fra EU til USA under EU's og USA's værn om privatlivets fred, til det strengt nødvendige med henblik på at nå det tilsigtede mål"[38].

Ved hjælp af rammerne, der er fremsat i afsnit 1.2 i denne udtalelse, og under hensyntagen til de amerikanske myndigheders fremstillinger og Kommissionens konklusioner har WP29 vurderet de nuværende retslige rammer og amerikanske efterretningsbureauers fremgangsmåder samt de forhold, hvorunder de tillader indblanding i de grundlæggende rettigheder, hvad angår privatliv og databeskyttelse som beskyttet under de europæiske retslige rammer. Denne vurdering er baseret på analysen i Presidential Policy Directive 28

[38] Udkastet til Kommissionens afgørelse i henhold til Europa-Parlamentets og det Europæiske Råds direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der ydes af EU's og USA's værn om privatlivets fred, § 75.

(PPD-28), Dekret 12333 (EO12333) og på forskellige retslige grundlag fastsat af Foreign Intelligence Surveillance Act (FISA - afsnit 104, afsnit 402, afsnit 215, afsnit 501 og afsnit 702). WP29 har henholdt sig til bilag VI i værnet om privatlivets fred, som består af et brev udarbejdet af Office of the Director of National Intelligence (ODNI) vedrørende sikkerhedsforanstaltninger og begrænsninger, der er gældende for amerikanske myndigheder for national sikkerhed, og som opsummerer de oplysninger, der er blevet fremlagt for Europa-Kommissionen vedrørende indsamlingen af signalefterretninger i USA.

3.2 Garanti A – Behandling skal være i overensstemmelse med loven og baseret på klare, præcise og forståelige regler

I henhold til europæisk lov skal en indblanding være i overensstemmelse med love, veletablerede politikker og procedurer samt være tilstrækkeligt klare og forståelige (inden for den diskretionsmargin, der tilkendes individuelle lande) for at give borgere en tilstrækkelig tilkendegivelse, hvad angår de omstændigheder og forhold, hvorunder offentlige myndigheder er bemyndiget til at gribe til overvågningsmetoder[39].

WP29 anfører, at signalefterretningsaktiviteter udføres på grundlag af en tilgængelig retslig ramme. Alle love, der er nævnt i bilag VI (PPD-28, FISA, USA FREEDOM ACT, FOIA) er tilgængelige for offentligheden online (i og uden for USA). Bilag VI fremsætter et resumé over den regulerende, retslige ramme, indsamlingsbegrænsningerne, fastholdelses- og udbredelsesbegrænsningerne, overholdelse samt tilsyn, gennemsigtighed og afhjælpning. Det amerikanske retssystem til efterretningsaktiviteter består af flere forskellige dokumenter, inklusive individuelle bureauers rapporter, politikker og procedurer, som skal analyseres for at få en bedre forståelse af, hvordan aktiviteterne udføres, både teoretisk og i praksis. I denne henseende har WP29 koncentreret sig om et begrænset antal punkter, som den anser som afgørende.

3.2.1 Dekret 12333 og Presidential Policy Directive 28

Anvendelsesområdet for EO12333 er bredt; i princippet kan alle udenlandske efterretningstjenesters dataindsamling finde sted ud fra den amerikanske præsidents skøn baseret på dekretet. Det er imidlertid blevet argumenteret, at siden indførelsen af FISA kan EO12333 kun anvendes til indsamling af data uden for det amerikanske område. WP29 anfører, at EO12333 ikke kommer med mange oplysninger vedrørende dens geografiske anvendelsesområde, det omfang, hvori data kan indsamles, opbevares eller udbredes yderligere, eller om forseelsernes natur, der kan give anledning til overvågning, eller den slags oplysninger, der kan indsamles eller anvendes.

[39] ECtHR Zakharov § 247 "Retten har tidligere konstateret, at lovkravet om "adækvans" ikke går så langt som til at tvinge staterne til at vedtage retsbestemmelser, der detaljeret anfører al adfærd, som kan afstedkomme en beslutning om at gøre en fysisk person genstand for en hemmelig overvågning af årsager, der involverer "national sikkerhed". Afhængigt af omstændighederne kan trusler over for national sikkerhed svinge i natur og kan være uventede eller vanskelige at definere på forhånd (se Kennedy, anført ovenfor, § 159). Samtidig har retten også understreget, at i sager, der påvirker grundlæggende rettigheder, ville den være i strid med retssamfundet, ét af de elementære principper ved et demokratisk samfund nedfældet i konventionen, for et skøn, der er tilstået den udøvende myndighed inden for området med national sikkerhed, og som skal udtrykkes med hensyn til fri bemyndigelse. Derfor skal loven angive anvendelsesområdet for alle sådanne skøn, der tildeles de kompetente myndigheder, og måden for dens udførelse med tilstrækkelig klarhed, hvor der tages hensyn til det lovlige mål for den pågældende metode, for at give den fysiske person tilstrækkelig beskyttelse mod arbitrær indblanding."

Efter WP29's opfattelse er det primære formål ved Presidential Policy Directive 28 (PPD-28) at fastsætte grænserne for indsamlingen og behandlingen af persondata, uanset hvilket overvågningsprogram der anvendes, og hvorfra data blev skaffet.

PPD-28 er et direktiv fra den amerikanske præsident, der fastlægger overensstemmelsesprincipperne, ud fra hvilke signalefterretningsindsamlingen skal bemyndiges og udføres, men PPD-28 er ikke et retsligt grundlag for indsamling. PPD-28 er effektiv, idet den indfører disse principper blandt efterretningsfællesskabers instanser, så de kan implementere dem i deres politikker og procedurer. Direktivet gælder for signalefterretningsaktiviteter, uanset stedet for dataene på det tidspunkt, hvor de bliver indsamlet, i og uden for USA. Derfor gælder det for de data, der indsamles til signalefterretningsformål, når de videregives fra EU til USA.

PPD-28 anfører især, at signalefterretningsaktiviteter skal være så tilpassede, som det er muligt[40]. Vedrørende brugen af dataene fastlægger den procedurer til dataminimering (inklusive betingelser for opbevaring og udbredelse af dataene), datasikkerhed og relevant personales aktindsigt [dvs. regler, der omfatter sikkerhedsforanstaltninger, som begrænser risiciene for misbrug og forkert brug], datakvalitet og tilsyn. Disse garantier gælder uanset de registreredes nationalitet, dvs. for amerikanske og ikke-amerikanske personer.

Under videregivelse af dataene til USA er de sikkerhedsforanstaltninger, der er fastsat af PPD-28, også gældende. Bilag VI indeholder en forpligtelse fra ODNI's side, at hvis det amerikanske efterretningsfællesskab skulle indsamle data fra transatlantisk kommunikation, mens de videregives til USA, "ville det ske underlagt begrænsningerne og sikkerhedsforanstaltningerne fremsat heri, inklusive kravene i PPD-28"[41]. WP29 anfører, at der fortsat er en mangel på veletableret retslære, som fastsætter lovligheden ved kommunikationsopsnapning, hvis den skulle udføres af et vilkårligt land. Under alle omstændigheder hverken bekræfter eller afviser USA, at de bruger kommunikationsopsnapning som en metode til indsamling af efterretningsdata.

Begrebet "signalefterretning" er hverken defineret i PPD-28 eller i nogen anden relevant tekst.

3.2.2 Foreign Intelligence Surveillance Act

FISA's tekst lader generelt set til at være klarere og mere præcis. Tolkningen af mange bestemmelser i lyset af PPD-28 og dermed deres praktiske gyldighed afhænger imidlertid i stor udstrækning af implementeringen foretaget af de forskellige bureauer. Mens en fuld rapport over implementeringen af de nye sikkerhedsforanstaltninger endnu ikke er tilgængelig, har amerikanske delegater informeret WP29's repræsentanter om, at implementeringen af sikkerhedsforanstaltningerne i PPD-28 rent faktisk er blevet fuldført og udføres på en tilsvarende måde i hele det amerikanske efterretningsfællesskab.

[40] "Signalefterretningsaktiviteter skal være så tilpassede, som det er muligt. Når det skal fastslås, om signalefterretning skal indsamles, skal USA tage højde for tilgængeligheden af andre oplysninger, inklusive fra diplomatiske og offentlige kilder. Sådanne passende og mulige alternativer til signalefterretning bør prioriteres." (Afsnit 1(d)).

[41] Værnet om privatlivets fred, bilag VI, brevet fra Office of the Director of National Intelligence (ODNI) vedrørende sikkerhedsforanstaltninger og begrænsninger, der er gældende for amerikanske myndigheder for national sikkerhed, punkt 2.

Mere præcist står afsnit 501 relativt klart vedrørende den slags efterretningsaktiviteter, der kan fås mandat til: "Produktionen af materielle ting (inklusive bøger, fortegnelser, papirer, dokumenter og andre elementer)". Det bør imidlertid anføres, at det faktum, at definitionen af "materielle ting" omfatter "andre elementer", gør anvendelsesområdet for denne myndighed temmelig bredt.

Afsnit 702, som tillader, at data, der skal indsamles fra ikke-amerikanske personer, som med rimelighed menes at befinde sig uden for USA, for at få fat i udenlandske efterretningsoplysninger[42], ikke fremsætter samme detaljerede niveau som afsnit 501. Vedrørende dets anvendelsesområde er afsnit 702 rettet mod serviceudbydere af elektronisk kommunikation, der er veletablerede i USA til indsamling af udenlandske efterretningsoplysninger om fysiske personer, der befinder sig uden for USA. Definitionen "udenlandske efterretningsoplysninger" er bred. Den omfatter blandt andet "oplysninger angående en udenlandsk magt eller et udenlandsk område, der vedrører udførelsen af USA's udenrigsanliggender"[43], og som bringer nogen uvished op, hvad angår den type oplysninger, der kan indsamles i praksis.

På trods af afklassificeringen af dokumenter forbliver rapporter til Kongressen og tilsynsrapporterne fra Privacy and Civil Liberties Oversight Board (i det følgende benævnt: PCLOB), FISA's gyldighed, inklusive anvendelsesområdet og anvendelsen af de specificerede valgbegreber uklare og forvirrende. Der henvises til anvendelsen af specificerede valgbegreber ("tildelte selektorer") i en PCLOB-rapport[44], men det er WP29's opfattelse, at det ikke svarer til de målrettende regler i afsnit 702[45]. Der henvises ikke generelt til dem som tilgængelige regler, så vidt WP29 har været i stand til at bekræfte.

3.2.3 Konklusion

Generelt set anfører WP29, at de relevante tekster vedrørende efterretningsaktiviteter er tilgængelige online, og at de amerikanske myndigheder har taget flere vigtige skridt hen imod gennemsigtighed.

WP29 anerkender, at der siden 2013 er blevet publiceret et stort antal dokumenter, såsom politikker, procedurer, FISC-beslutninger og andre afklassificerede dokumenter. Endvidere har PCLOB udgivet vigtige rapporter om de aktiviteter, der udføres på grundlag af afsnit 702 og USA FREEDOM Act. En lignende rapport forventes udarbejdet om aktiviteter under EO12333.

Flere lovgivningsbilag, der kunne kaste lys over betydningen af dekretet om fysiske personer uden for USA og andre gældende sikkerhedsforanstaltninger, er klassificerede og derfor ikke tilgængelige for offentligheden eller fysiske personer, som eventuelt er påvirket af deres gyldighed. Hvor tekster er blevet afklassificeret, fremsætter de kun begrænset værdi og indblik, hvad angår efterretningsaktiviteter.

[42] 50 U.S. Code § 1881a (D)(1).
[43] 50 U.S. Code § 1801 (e) (2).
[44] PCLOB-rapporten om overvågningsprogrammet, der drives i henhold til afsnit 702 FISA, punkt 32.
[45] 50 U.S. Code § 1881a(D).

På trods af de bestræbelser, der er gjort for at forklare EO12333's virkemåde efter Snowden-afsløringerne, særligt gennem vedtagelsen af PPD-28, forbliver den aktuelle, praktiske anvendelse af EO12333 uklar. WP29 anfører, at bilag VI til værnet om privatlivets fred ikke fremsætter detaljerede oplysninger om EO12333's funktion.

WP29 glæder sig over de begrænsninger, som er indført med PPD-28, men finder det vanskeligt at vurdere, om den retlige amerikanske ramme for overvågningen er tilstrækkelig forudsigelig, dvs. indeholder "tilstrækkelig[e] indikation[er] af, under hvilke omstændigheder og på hvilke betingelser offentlige myndigheder har kompetence til at anvende sådanne foranstaltninger", da yderligere afklaring, herunder offentliggørelsen af PCLOB-rapporten i EO12333, afventes.

3.3 Garanti B – Nødvendighed og proportionalitet i forbindelse med de lovlige mål, der tilstræbes, skal vises

3.3.1 Presidential Policy Directive 28

PPD-28 introducerede begrænsninger vedrørende de formål, hvortil persondata kan anvendes, og for de betingelser, hvorunder de kan udbredes og påvirker indsamlingen af signalefterretning, uanset hvilket retsligt grundlag der anvendes.

Særligt anfører afsnit 1 i PPD-28, at amerikanske signalefterretningsaktiviteter altid skal være "så tilpassede, som det er muligt". Mens denne begrænsning anerkendes, er det vanskeligt at fastslå, om "så tilpasset, som det er muligt" betyder, at hele dataindsamlingen er nødvendig og proportional.

PPD-28 anerkender, at masseindsamling fortsat er tilladt "for at identificere nye eller opstående trusler og andre afgørende oplysninger om national sikkerhed, der ofte er skjult i det store og komplekse system med moderne global kommunikation"[46]. WP29 anfører, at PPD-28 fremsætter, at "signalefterretning, der er indsamlet "i stor mængde" betyder den autoriserede indsamling af store mængder signalefterretningsdata, der, som følge af tekniske eller driftshensyn, anskaffes uden anvendelse af diskriminanter (f.eks. bestemte identifikatorer, valgbegreber osv.)".

PPD-28 indfører grænser for anvendelsen af signalefterretning, der indsamles i stor mængde, hvad angår anvendelsesformålet. De seks formål, hvortil data kan indsamles "i stor mængde", inklusive kontraterrorisme og andre former for alvorlige (transnationale) forbrydelser. WP29's analyse tyder på, at formålsbegrænsningen er temmelig bred (og muligvis for bred) til at kunne anses som målrettet.

PPD-28 udelukker ikke muligheden for vilkårlig indsamling af personoplysninger i stor mængde, ligesom omfanget af sådanne muligheder for indsamling fortsat er uklart og meget vidtrækkende. I denne henseende anfører WP29, at ODNI i bilag VI stadfæster, at "alle

[46] PPD-28, afsnit 2 og værnet om privatlivets fred, bilag VI, brevet fra Office of the Director of National Intelligence (ODNI) vedrørende sikkerhedsforanstaltninger og begrænsninger, der er gældende for amerikanske myndigheder for national sikkerhed, punkt 3.

masseindsamlingsaktiviteter vedrørende internetkommunikation, som det amerikanske efterretningsfællesskab udfører gennem signalefterretning, er baseret på en lille del af internettet[47] og vil derfor værdsætte yderligere dokumentationsmateriale, der tilvejebringes gennem gennemsigtighedsforanstaltninger.

3.3.2 Foreign Intelligence Surveillance Act

Afsnit 215 og afsnit 702 i FISA's minimeringsprocedurer blev indført for at beskytte amerikanske personer mod vidtspændende statsadgang til deres data. Disse begrænsninger gælder ikke officielt for udlændinge, selvom amerikanske embedsmænd gentagne gange har tilkendegivet på både offentlige og private møder med WP29-repræsentanter, at anvendelsesområdet for gyldigheden af minimeringsprocedurer sidenhen i praksis er blevet udvidet til at dække alle personer, uanset deres nationalitet eller normale bopælssted.

Afsnit 702 præciserer, at en autoriseret indsamling "skal udføres i overensstemmelse med artikel 4 i USA's forfatning, og begrænser dataindsamling til, hvad der betragtes som værende i overensstemmelse med princippet om passende søgning. I denne henseende skelnes der ikke mellem amerikanske og ikke-amerikanske virksomheder". Med andre ord ville "masseindsamling", der finder sted i USA, på den betingelse, at den fjerde forfatningsændring gælder for alle data indsamlet i USA, være "urimeligt" og dermed forfatningsstridig.

WP29 anerkender, at konklusionerne i PCLOB-rapporten om, at "i praksis drager "ikke-amerikanske personer" også fordel af aktindsigts- og opbevaringsbegrænsningerne, som pålægges de forskellige bureauers minimerings- og/eller målretningsprocedurer som følge af omkostningen og vanskeligheden ved at identificere og fjerne amerikanske personoplysninger for en stor datamængde, betyder, at hele datasættet typisk set håndteres i overholdelse af de højere amerikanske datastandarder".

WP29 anfører endvidere, at i henhold til PCLOB-konklusionerne "fungerer programmet ikke ved at indsamle kommunikation i stor mængde". Den statistiske gennemsigtighedsrapport 2014 udgivet af ODNI bekræfter denne konklusion. I henhold til PCLOB-rapporten anvendes der også "tildelte selektorer", såsom en e-mailadresse eller et telefonnummer, til at gøre overvågningen målrettet[48].

De tilsvarende, tilgængelige offentlige regler vedrørende målretning fremsætter imidlertid ikke sådanne målrettede regler, og tilstræber kun at undgå at gøre amerikanske personer eller personer, som er hjemmehørende i USA, til mål. Endvidere er fordelene, som ifølge PCLOB i praksis gælder for ikke-amerikanske personer, ikke juridisk bindende eller lovmæssigt fastsat, da den tilgængelige lovgivning vedrørende målretning ikke fremsætter sådanne målrettede

[47] Værnet om privatlivets fred, bilag VI, brevet fra Office of the Director of National Intelligence (ODNI) vedrørende sikkerhedsforanstaltninger og begrænsninger, der er gældende for amerikanske myndigheder for national sikkerhed, punkt 4; i denne henseende minder WP29 om rapporten om konklusionerne fra de europæiske medformænd for ad hoc-arbejdsgruppen for EU og USA om databeskyttelse, der fremsætter, at "kommunikationsdata udgør en meget lille del af global internettrafik", i lyset af at "langt størstedelen af global internettrafik består af store mængder streaming og downloads såsom tv-serier, film og sport" (§3.1.2 i rapporten)44.
[48] PCLOB-rapporten om overvågningsprogrammet, der drives i henhold til afsnit 702 FISA, punkt 32.

regler og kun tilstræber at undgå at gøre amerikanske personer eller personer, som er hjemmehørende i USA, til mål.

WP29 minder også om, at til formål med afsnit 702 er personer ikke blot fysiske personer, men også grupper, enheder, sammenslutninger, virksomheder eller udenlandske magter. Det faktum, at indsamling er berettiget ved, "at et væsentligt formål ved anskaffelsen er at få udenlandske efterretningsoplysninger", giver også nogen uvished hvad angår dens formål og nødvendighed. WP29 anerkender imidlertid, at oplysningerne, som er fremsat i bilag VI, om at det samlede antal tilsigtede fysiske personer under afsnit 702 i 2014 var ca. 90.000 fysiske personer[49]. Den første evaluering af værnet om privatlivets fred vil give mulighed for yderligere dokumentationsmateriale på målretningsreglerne, som skal vises.

Indtil videre er der ingen endegyldig retslære om lovgyldigheden ved enorme og vilkårlige dataindsamlinger og efterfølgende anvendelse af persondata til det formål at bekæmpe kriminalitet, inklusive spørgsmålet om under hvilke omstændigheder sådan indsamling og anvendelse af persondata kan finde sted. EU-Domstolen forventes at tage sig af dette spørgsmål, i det mindste i en vis udstrækning, i løbet af 2016, både de forenede sager Tele2 Sverige AB mod Post- och telestyrelsen og Secretary of State for the Home Department mod Davis og andre[50] i den rådgivning, der skal gives vedrørende gyldigheden af PNR Canada-aftalen[51]. I mellemtiden minder WP29 om, at den hele tiden har ment, at enorm og vilkårlig dataindsamling under ingen omstændigheder kan anses som proportional[52].

3.3.3 Konklusion

På trods af de begrænsninger, der fulgte efter introduktionen af PPD-28, har WP29 fortsat bekymringer, især vedrørende dataindsamlingens proportionalitet. For det første er der tegn på, at USA fortsat indsamler enorme og vilkårlige data eller i det mindste ikke udelukker, at de stadig kan gøre det i fremtiden. WP29 har hele tiden fastholdt, at sådan dataindsamling ikke er i overensstemmelse med EU-lovgivning og derfor ikke er acceptabel.

For det andet anfører WP29, at også målrettet databehandling eller behandling, der er "så målrettet som muligt", stadig kan anses som værende enorm. Uanset om sådan enorm dataindsamling skal tillades eller ej er i øjeblikket ikke underlagt retsprocesser for EU-Domstolen. Derfor vil WP29 ikke foretage en endelig vurdering, hvad angår lovgyldigheden af målrettet, men enorm, databehandling. Det understreges imidlertid, at hvis målrettet, men enorm, databehandling tillades, skal principperne for målretning gælde for både indsamlingen og den efterfølgende anvendelse af dataene og kan ikke blot begrænses til anvendelsen. Under alle omstændigheder er der behov for en afklaring i udkastet til tilstrækkelighedsafgørelsen, hvad angår de seks formål nævnt i PPD-28, hvortil data kan indsamles "i store mængder". WP29 er på nuværende tidspunkt ikke overbevist om, at disse formål er tilstrækkeligt

[49] Bilag VI, punkt 11.
[50] EU-Domstolen, forenet sag C-203/15 og C-698/15.
[51] EU-Domstolen, sag A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

begrænsede for at sikre, at dataindsamling rent faktisk er begrænset til det, som er nødvendigt og proportionalt.

3.4. Garanti C - Der skal være en uafhængig tilsynsmekanisme

USA har ikke én enkelt tilsynsinstans på føderalt niveau, som har til opgave at føre tilsyn med konsekvenser af efterretnings- og overvågningsprogrammer på privatlivets fred og databeskyttelse. I stedet er amerikanske efterretningsaktiviteter genstand for en flerlaget tilsynsproces: Der kan skelnes mellem internt og eksternt tilsyn. WP29 anerkender, at de amerikanske tilsynsinstansers rapporteringspraksis er meget detaljeret og for det meste offentlig.

3.4.1 Internt tilsyn

Alle efterretnings- og sikkerhedsbureauer har medarbejdere, der er ansvarlige for at sikre overholdelse af deres lovgivningsramme inklusive generalinspektører, hvis primære opgave er at vurdere bureauarbejdets overholdelse af lovgivningen, inklusive, men ikke begrænset til de love, som vedrører privatlivets fred og databeskyttelse. Generalinspektørerne fastslås ved vedtægt og alle er (eller vil snart være) beskikket af præsidenten efter bekræftelse fra senatet i et forsøg på sikre, at de vil være organisatorisk uafhængige og rapportere til Kongressen. Derfor mener WP29, at generalinspektørerne sandsynligvis opfylder kriteriet for organisatorisk uafhængighed som defineret af EU-Domstolen og den Europæiske Menneskerettighedsdomstol (ECtHR), i det mindste fra det øjeblik, hvor den nye udnævnelsesproces gælder for alle. I øjeblikket er der fortsat nogle bekymringer vedrørende generalinspektørerne, som stadig udpeges af direktøren for det bureau, de har tilsyn med.

Generalinspektøren kan komme med anbefalinger, som derefter kan henvises til justitsministeriet og til PCLOB eller endda til Kongresudvalget, som kan indføre anbefalingerne. Hvis generalinspektøren konstaterer en overtrædelse, kan den håndteres gennem interne foranstaltninger og politikker og rapporteres til Kongressen. Generalinspektøren har for eksempel bemyndigelsen til at udføre både revisioner og inspektioner.

WP29 anfører, at generalinspektørens rapporter kan holdes tilbage fra offentligheden, og at generalinspektøren også kan forhindres i at rapportere dem, hvis de kontrollerede oplysninger er klassificerede. Rapporterne vil imidlertid hele tiden være underlagt Kongressens tilsyn, som er en essentiel sikkerhedsforanstaltning, selv hvis den ikke giver grundlag for individuel regres.

Alle bureauer har medarbejdere inden for privatlivets fred og borgerrettigheder, som hjælper med det obligatoriske selvrapporteringssystem under Kongressens tilsyn.

Generelt set kan de interne tilsynsmekanismer, der er på plads, anses som temmelig robuste; for at retfærdiggøre et indgreb i de grundlæggende rettigheder til privatlivets fred og databeskyttelse skal opsyn imidlertid være helt uafhængigt. Og mens WP29 respekterer og påskønner de forskellige medarbejdere inden for privatlivets fred og borgerrettigheders

arbejdet, kan den ikke udlede, at de imødekommer det påkrævede uafhængighedsniveau for at fungere som en uafhængig tilsynsførende.

3.4.2 Eksternt tilsyn

Eksternt tilsyn består af flere forskellige mekanismer: retsligt tilsyn under afsnit 501 og 702 tilsikret af FISA-domstolen (i det følgende benævnt: FISC), tilsyn fra Kongressens udvalgte efterretningskomitéer og de opgaver, der udføres af PCLOB.

WP29 minder om, at tilsynet ideelt, som det også er blevet fremsat af EU-Domstolen og ECtHR, bør være under en dommers bemyndigelse for at garantere, at proceduren er uafhængig og upartisk. Indtil for nylig var FISC-proceduren en ex parte-procedure, uden mulighed for de involverede fysiske personer at blive hørt eller endda at kende til sagen. Nu om stunder forbliver FISC-proceduren desuden ex parte, men efter vedtagelsen af USA FREEDOM Act blev amici curiae til FISC indført. Amici curiae fungerer uafhængigt, men er ikke fastsat for at forsvare specifikke fysiske personer, der kan være involveret i sagen.

USA Freedom Act oprettede en gruppe med amici curiae til at briefe FISC om vigtige sager. Domstolen har valgt fem advokater, som har fået de relevante sikkerhedsgodkendelser, og som kommer med tekniske råd, deltager i FISC-retsmøder og udleverer sagsresuméer samt anfører en sag på realiteten fra et perspektiv med privatlivets fred og borgerrettigheder. De vil imidlertid kun gøre det i vigtige sager, eller når nye juridiske spørgsmål opstår[53].

Afsnit 215 er nærmest helt underlagt ex ante (men ikke ex post) retsligt tilsyn, eftersom alle programmer, der anvender afsnit 215 som grundlag for indsamling, er afhængige af godkendelse fra FISC. PCLOB-rapporten angiver, at "afsnit 702 afviger fra den traditionelle FISA-ramme for elektronisk overvågning både i de anvendte standarder og i manglen på individualiserede afgørelser fra FISC. I henhold til vedtægten foretager den amerikanske justitsminister og Director of National Intelligence årlige certificeringer, der autoriserer, at ikke-amerikanske personer, som med rimelighed menes at befinde sig uden for USA, bliver mål for anskaffelsen af udenlandske efterretningsoplysninger, uden at der præciseres over for FISC, hvilke bestemte ikke-amerikanske personer der vil være målet. […] Der er heller intet krav om, at regeringen påviser bestyrket mistanke om, at et mål i henhold til afsnit 702 er en udenlandsk magt eller repræsentant for en udenlandsk magt, som det er påkrævet under traditionel FISA"[54].

Inden for Kongressen har de udvalgte efterretningskomitéer også en tilsynsopgave med at godkende efterretningsaktiviteter, især gennem budgetforslaget. Senat og House Intelligence Committees modtager klassificerede briefinger om efterretningsaktiviteter. Den amerikanske justitsminister skal rapportere til disse komitéer hver sjette måned om FISA's elektroniske overvågning. Det forbliver uklart for WP29, i hvilket omfang de er i stand til at diskutere behandlingen af individuelle personers persondata, især ikke-amerikanske personers.

[53] Freedom Act BENÆVNELSE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT'S REFORMER afsnit 401. Udnævnelse af amici curiae.
[54] PCLOB-rapporten om overvågningsprogrammet i henhold til afsnit 702 FISA, punkt 24, 25.

PCLOB er en uafhængig del af den ledende sektor inden for den amerikanske regering, som er udstyret med to grundlæggende bemyndigelser: (1) at evaluere og analysere handlinger, som den ledende sektor udfører for at beskytte nationen [USA] mod terrorisme, idet det sikres, at der er balance mellem behovet for sådanne handlinger og behovet for at beskytte privatlivets fred og borgerrettigheder, og (2) at sikre, at der tages behørig højde for bekymringer om frihed i udformningen og implementeringen af love, bestemmelser og politikker vedrørende bestræbelserne på at beskytte nationen mod terrorisme. WP29 anfører, at PCLOB har indstævningsmagt og aktindsigt i klassificerede oplysninger. Under udførelse af sin opgave tjekker den også programmernes virkekraft. Det tilsyn udføres ikke inden, men efter faktum. PCLOB har udvist sine uafhængige beføjelser ved at være uenig med den amerikanske præsident i retslige anliggender. Navnlig mente den, at afsnit 215 programmet med telefonmetadata ikke var retsligt bemyndiget og konkluderede, at det ikke var effektivt, da der ikke var bevis på forstyrrende angreb. PCLOB foretog også en årelang undersøgelse af 702-programmet og konstaterede, at det var lovligt og klart autoriseret ved vedtægt, og at afsnit 702 har vist sig at være meget effektiv, inklusive i forbindelse med terrorisme-relaterede anliggender. Til sidst fulgte den kravet om gennemsigtighed og konstaterede, at flere klassificerede fakta ikke behøvede at være klassificerede. PCLOB menes at rapportere om implementeringen af PPD-28 i nærmeste fremtid. I denne henseende mener den, at for at opbevare oplysninger om en udlænding er det simple faktum, at den person er udlænding, ikke nok.

Endelig anfører WP29, at EO12333 ikke fremsætter nogen retslige evaluerings-, tilsyns- eller afhjælpningsmekanismer til overvågningsprogrammerne, der udføres på grundlag heraf.

3.4.3 Konklusion

Udkastet til tilstrækkelighedsafgørelsen viser, at en flerlaget tilgang til både interne og eksterne tilsynsmekanismer er på plads i USA. Selvom tilsynsmekanismernes virkemåde kan være forvirrende, er WP29 overbevist om, at der generelt er tilstrækkelige interne tilsynsmekanismer på plads. WP29 er imidlertid bekymret over, at der er utilstrækkeligt tilsyn med overvågningsprogrammerne, som udføres på grundlag af EO12333.

WP29 anfører, at dens tidligere kritik med, at procedurerne foran FISC ikke er fjendtlige, kun er blevet nedsat i et vist omfang ved at indføre amici curiae, som har til opgave at "fremme beskyttelsen af individuelt privatliv og individuelle borgerrettigheder". Desuagtet sørger FISC ikke for noget effektivt, retsligt tilsyn med målretningen af ikke-amerikanske personer. Der er fortsat nogen tvivl vedrørende FISC's evne til effektivt at vurdere målretnings- og minimeringsprocedurerne, som det også var anført af PCLOB[55].

[55] PCLOB-rapporten om overvågningsprogrammet, der drives i henhold til afsnit 702 FISA, punkt 11.

3.5 Garanti D - Effektive retsmidler skal være tilgængelige for den fysiske person

3.5.1 Retsmidler

3.5.1.1 Krav til søgsmålskompetence

Det amerikanske system vedrørende retsmidler omfatter en vigtig grænse: Den amerikanske forfatning pålægger en fysisk person at påvise, at han har søgsmålskompetence: "Kravet om, at sagsøgerne har lidt eller vil lide direkte skade, og at denne skade kan afhjælpes. På føderalt niveau kan søgsmål ikke bare anlægges på det grundlag, at en fysisk person eller en gruppe er utilfredse med en regeringshandling eller lov"[56]. Sådant krav lader til at være erklæret ugyldigt af manglen på meddelelse til fysiske personer, der er genstand for overvågning, selv efter disse foranstaltninger er ophørt. EU-Domstolen og ECtHR har gentagne gange fremsat, at fysiske personer skal kunne få adgang til administrativ eller retslig afhjælpning. ECtHR har i sin Zakharov-beslutning bekræftet, at baseret på retslære kan alle henvende sig til retten, hvis de har legitim årsag til at mistænke et indgreb i deres grundlæggende rettigheder[57].

Endvidere tilbydes udlændinge uden for USA ikke fuld forfatningsmæssig beskyttelse i USA efter retslære fra højesteretten i USA[58]. Dette er især sandt i forbindelse med den fjerde forfatningsændring, som beskytter amerikanske statsborgere – men ikke ikke-amerikanske personer – mod unødvendige gennemsøgninger og beslaglæggelser, og hvoraf megen af den amerikanske ret til privatlivets fred stammer. Europæiske statsborgere og andre europæiske personer, der bor uden for USA, er simpelthen ekskluderet fra beskyttelsen fra den fjerde forfatningsændring[59].

Den begrænsede anvendelse af loven om retslig afhjælpning (både hvad angår hovedindholdet, da det ekskluderer national sikkerhed, men også vedrørende de personer, som kan støtte sig til loven), de mange undtagelser og den retslige usikkerhed vedrørende de bureauer, som loven om retslig afhjælpning vil gælde for, opfylder ikke kravet om at tilbyde en effektiv afhjælpningsmekanisme til alle fysiske personer, der er involveret i sager med efterretningsovervågning af national sikkerhed.

3.5.1.2 Presidential Policy Directive 28

WP29 anfører, at PPD-28 kun er et direktiv og derfor ikke kan generere nogen rettigheder for fysiske personer. Dette kan kun gøres gennem lovgivning. Derfor kan fysiske personer ikke henvende sig til retten baseret på en hævdet overtrædelse af sikkerhedsforanstaltningerne i PPD-28.

---

[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper mod Amnesty International USA.
[57] ECtHR, Zakharov, § 171.
[58] USA mod Verdugo - Urquidez, punkt 264-266.
[59] Europæiske medformænds rapport, afsnit 2.

3.5.1.3 Foreign Intelligence Surveillance Act

I henhold til FISA er der nogle retsmidler for fysiske personer i tilfælde af ulovlig overvågning. Ifølge FISA "skal en forurettet person, bortset fra henholdsvis en udenlandsk magt eller en repræsentant fra en udenlandsk magt [...], som har været genstand for en elektronisk overvågning, eller om hvem oplysninger opnået via elektronisk overvågning af sådan person er blevet offentliggjort eller anvendt i strid med afsnit 1809 i denne adkomst, have søgsmålsgrundlag mod enhver person, der har begået sådan overtrædelse". Dette ekskluderer imidlertid udtrykkeligt den udenlandske magt eller repræsentanten for en udenlandsk magt, der var genstand for dette. Som allerede anført vil sagsøgeren ikke desto mindre skulle påvise, at han har søgsmålskompetence, hvilket ikke vil være muligt i praksis.

USA Freedom Act har oprettet en Amicus Curiae-rådgivningskomité til FISA-domstolen til at give (frivillig) rådgivning i tilfælde af væsentlige, nye, retslige tolkninger. Deres opgave er imidlertid at komme med upartiske råd og ikke at forsvare en bestemt fysisk persons interesser efter dennes anmodning.

3.5.2 Administrative retsmidler

3.5.2.1 Generalinspektører

En anden vej til retsmidler er at gå gennem generalinspektøren, som en klage kan indgives til. Generalinspektøren har imidlertid ikke nogen forpligtelse til at se på hver enkelt klage: Der er ingen ret til at blive behandlet, men nærmere en skønsmæssig beføjelse. Generalinspektøren kan også udsende rapporter med konklusioner på overtrædelser, hvor oplysninger er afklassificerede. I tilfælde af, at en fysisk person kan formode, at rapporten påvirker ham/hende, så vil han/hun være i stand til at henvende sig til retten på det grundlag, at en lovovertrædelse konkluderes.

3.5.2.2 Freedom of Information Act

Et retsmiddel, der er tilgængeligt for alle personer, er indgivelsen af anmodning om oplysningsfrihed, baseret på Freedom of Information Act (FOIA). Ifølge den amerikanske regering kan en FOIA-anmodning generelt fremsættes af alle personer – amerikansk statsborger eller ej – ved blot at bede om et bureaus fortegnelser. Det omfatter fortegnelser om den fysiske person, selvom vedkommende i sådant tilfælde pålægges at fremlægge certificering af identitet. Hvis oplysningerne er klassificerede for at beskytte national sikkerhed, er det imidlertid usandsynligt, at en FOIA-anmodning vil blive bevilliget, da en undgåelse er gældende: Bureauer er ikke forpligtet til at give indsigt i klassificerede oplysninger, inklusive hvis disse oplysninger vedrører den fysiske person, som har fremsat anmodningen. Oplysninger fra igangværende retshåndhævelsesefterforskninger er fuldstændigt ekskluderet fra FOIA-anmodninger. Til sidst fremsætter FOIA-anmodningen, efter WP29's mening, ikke en ret til at få lovgyldigheden af behandlingen kontrolleret af en uafhængig myndighed.

3.5.3 Ombudsperson til værnet om privatlivets fred

3.5.3.1 Etablering af en ombudsperson

Værnet om privatlivets fred etablerer en ny mekanisme "til fysiske personer i Europa" til at indsende anmodninger vedrørende "USA's signalefterretning" til den nyligt oprettede ombudsperson til værnet om privatlivets fred. Stillingen som ombudsperson som forklaret i memorandummet, der er vedlagt brevet fra udenrigsministeren John Kerry, dateret 22. februar 2016, vil blive beklædt af understatssekretæren C. Novelli. Hun vil tage sig af dette funktionsområde foruden sin rolle som "senior koordinator for international diplomati vedrørende informationsteknologi", en stilling, der blev oprettet i afsnit 4, punkt d, i PPD-28. Det understreges i dette brev og i memorandummet, at "understatssekretæren rapporterer direkte til udenrigsministeren og er uafhængig fra efterretningsfællesskabet".

Til trods for dets navn forklares det i memorandummet, at ombudspersonen til værnet om privatlivets fred ikke kun vil behandle anmodninger vedrørende aktindsigt, der er videregivet fra EU til USA i henhold til værnet om privatlivets fred, i forbindelse med national sikkerhed, men også de anmodninger, hvor dataene er blevet videregivet i henhold til standard kontraktbestemmelser, bindende virksomhedsregler, undtagelsesbestemmelser (under artikel 26 i direktiv 95/46/EF) eller "eventuelle fremtidige undtagelsesbestemmelser" som defineret i fodnote 2 i memorandummet.

Den måde, hvorpå mekanismen formodes at fungere, kan opsummeres på følgende måde: En fysisk person i EU indsender en anmodning til en medlemsstats instans, som er kvalificeret til tilsynet af nationale sikkerhedstjenester, eller til en centraliseret "instans, der behandler klager fra fysiske personer i EU", i tilfælde af at sidstnævnte vil blive oprettet eller udpeget. Myndigheden, der videresender anmodningen til ombudspersonen, vil først skulle kontrollere, om anmodningen er fuldstændig, som defineret under brevets artikel 3, stk. b[60]. Når den er givet videre til ombudspersonen til værnet om privatlivets fred og konstateret at overholde artikel 3, stk. b, vil ombudspersonen til værnet om privatlivets fred komme med et svar, hvilket betyder, at han til sidst vil bekræfte, at "i) klagen er blevet ordentligt undersøgt, og at ii) de amerikanske love, vedtægter, dekreter, præsident-direktiver og bureaupolitikker, som fremsætter de begrænsninger og sikkerhedsforanstaltninger, der er beskrevet i brevet til Office of the Director of National Intelligence (ODNI), er blevet overholdt, eller i tilfælde af

[60] b. Instansen til håndtering af klager fra fysiske personer i EU vil, i overensstemmelse med følgende handlinger, sikre, at anmodningen er fuldstændig:
i) Ved at bekræfte, at den fysiske persons identitet, og at den fysiske person handler på egne vegne og ikke som en repræsentant for en statslig eller mellemstatslig organisation.
ii) Ved at sikre, at anmodningen foretages skriftligt, og at den indeholder følgende elementære oplysninger:
• alle oplysninger, der danner grundlaget for anmodningen,
• beskaffenheden af de oplysninger eller den afhjælpning, der søges,
• de amerikanske statsentiteter, der menes at være involveret, hvis nogen, og
• de andre metoder, der følges for at få de anmodede oplysninger eller afhjælpning samt det svar, der modtages gennem disse andre metoder.
iii) Ved at bekræfte, at anmodningen vedrører data, der med rimelighed menes at være blevet videregivet fra EU til USA i henhold til værnet om privatlivets fred, SCC'er, BCR'er, undtagelsesbestemmelser eller eventuelle fremtidige undtagelsesbestemmelser.
iv) Ved at komme med en foreløbig afgørelse om, at anmodningen ikke er ubetydelig, besværlig eller foretaget i ond tro.

manglende overholdelse at sådan manglende overholdelse er blevet afhjulpet"[61]. Svaret vil "hverken bekræfte eller afvise, om den fysiske person har været mål for overvågning, og ombudspersonen til værnet om privatlivets fred vil heller ikke bekræfte det specifikke retsmiddel, der blev anvendt"[62]. Hvad angår spørgsmålet, hvordan ombudspersonens undersøgelse udføres, bliver det forklaret, at ombudspersonen til værnet om privatlivets fred "vil arbejde tæt sammen andre amerikanske embedsmænd, inklusive relevante uafhængige tilsynsinstanser"[63], og mere specifikt "vil kunne koordinere tæt sammen med ODNI, justitsministeriet samt andre ministerier og bureauer, som er involveret i USA's nationale sikkerhed, som det er relevant, og generalinspektører, medarbejdere for Freedom of Information Act samt medarbejdere inden for borgerrettigheder og privatlivets fred"[64]. Denne koordinering skal være sådan for at sikre, at ombudspersonen til værnet om privatlivets fred kan sende et svar, inklusive bekræftelser som beskrevet ovenfor.

3.5.3.2 Vurderingen af den nye ombudspersonsmekanisme

Arbejdsgruppen anerkender de bestræbelser, som Europa-Kommissionen og den amerikanske regering har gjort sig med at indføre en ny mekanisme med det formål at forbedre mulighederne for retslig afhjælpning vedrørende amerikanske overvågningsaktiviteter. Den forstår, at vurderingen af denne mekanisme, som noget nyt inden for internationale relationer i forbindelse med signalefterretning eller national sikkerhed, er særlig vigtig.

I dette afsnit vil WP29 vurdere, hvordan etableringen af ombudspersonen til værnet om privatlivets fred vedrører de nødvendige krav til fysiske personer for at søge retslig afhjælpning, som det er fremsat i charteret, ECHR og de europæiske domstoles retslære.

3.5.3.3 Kan etableringen af en ombudsperson i sig selv være tilstrækkelig?

Til at begynde med skal der stilles det spørgsmål, om etableringen af en "ombudsperson" nogensinde kan anses som værende i overholdelse med charterets artikel 47 – som nævner et effektivt retsmiddel i en upartisk domstol[65] – i det mindste hvis der ikke er nogen anden tilgængelig måde til at søge effektiv, retslig afhjælpning. Dette er vigtigt, fordi EU-Domstolen i Schrems-sagen, i dens vigtige overvejelse 95, henviser til charterets artikel 47, og det gør den uden nogen tilkendegivelse af, at artikel 47 skal forstås med ændringer i konteksten med overvågningsmetoder. Tværtimod anvendte EU-Domstolen allerede charterets artikel 47 i Kadi II-sagen[66] til metoder til overvågning af henholdsvis national og international sikkerhed[67].

[61] Værnet om privatlivets fred, bilag III, afsnit 4, stk. e.
[62] Værnet om privatlivets fred, bilag III, afsnit 4, stk. e.
[63] Værnet om privatlivets fred, bilag III, afsnit 2, stk. a.
[64] Værnet om privatlivets fred, bilag III, afsnit 2, stk. a.
[65] I forklaringerne vedrørende charteret til grundlæggende rettigheder fremsættes det endvidere, at artikel 47 skal tolkes som en tilvejebringelse af en garanti for retten til et effektivt retsmiddel i en domstol (forklaring vedrørende charteret til grundlæggende rettigheder, forklaring af artikel 47 (2007/C303/02)).
[66] Forenede sager C-584/10 P, C-593/10 P og C-595/10 P, Europa-Kommissionen og Storbritannien mod Kadi, 18. juli 2013.
[67] Kadi II § 97 og 100: Alle Acts of Union, inklusive dem, som er udarbejdet til at gyldiggøre løsninger, der indføres af FN's sikkerhedsråd under charterets kapitel VII, er under evaluering for retmæssighed af domstolene i den Europæiske Union

ECtHR's retslære gør det imidlertid helt klart, at den retslige afhjælpning for ordinære domstole ikke er en betingelse for at anse overvågningsordninger som i overensstemmelse med artikel 8 (og artikel 13 i ECHR)[68]. I stedet har domstolen under artikel 8, som en nødvendig sikkerhedsforanstaltning til overvågningsaktiviteter, udviklet, at afhjælpning foran andre myndigheder kan være i orden. ECtHR har ikke desto mindre høje forventninger til andre myndigheder, som yder et effektivt retsmiddel, idet de anfører, at en sådan myndighed skal være "uafhængig af de myndigheder, som foretager overvågningen, og er udstyret med tilstrækkelige beføjelser og kompetence til at udvise effektiv og vedvarende kontrol"[69].

I Kennedy-sagen og Klass-sagen gav ECtHR et indblik i, hvad disse forventninger kan betyde i konteksten med hemmelig overvågning, når den registrerede ikke gøres opmærksom på behandlingen af dennes data. I begge disse domme anså ECtHR myndighederne for at være uafhængige, især uafhængige af de instanser, som foretog overvågningen, men også uafhængige af vejledningen[70] fra alle andre myndigheder. Nærmere betegnet i Kennedy-sagen godkendte domstolen en uafhængig og upartisk myndighed, som indførte sine egne procedureregler og bestod af medlemmer, der beklædte eller havde beklædt høje retsembeder eller var erfarne advokater[71].

I udførelsen af dens undersøgelse af fysiske personers klager havde myndighederne i begge domme desuden indsigt i alle relevante oplysninger, inklusive lukkede materialer. Endelig havde begge beføjelser til at afhjælpe manglende overholdelse[72].

Foruden spørgsmålet, om ombudspersonen kan anses som en "domstol", indebærer anvendelsen af charterets artikel 47, stk. 2, en yderligere udfordring, da den fremsætter, at domstolen skal være "fastsat ved lov". Det er imidlertid tvivlsomt, at et memorandum, som fremsætter en ny mekanismes virkemåde, kan anses som "lov".

Som en konsekvens – mens der huskes på princippet om essentiel ækvivalens – fremfor at vurdere, om en ombudsperson formelt kan anses som en domstol, der er fastsat ved lov, besluttede arbejdsgruppen at beskrive nuancerne ved retspraksis nærmere, hvad angår de specifikke krav, som er nødvendige for at overveje "retsmidler" og "retslig afhjælpning", som overholder de grundlæggende rettigheder i charterets artikel 7, 8 og 47 samt ECHR's artikel 8 (og 13). I sin yderligere analyse vil arbejdsgruppen, efter at have diskuteret den nye mekanismes anvendelsesområde, således fokusere på følgende kriterier: Kravet om at indsende en anmodning til ombudspersonen og om at modtage et svar ("søgsmålskompetence"), ombudspersonens uafhængighed, dens undersøgelsesbeføjelse til at tilgå de nødvendige materialer, inklusive klassificerede dokumenter, og om at anmode om

(kapitel VII vedrører søgsmål, hvad angår trusler mod freden, forstyrrelser af den offentlige ro og orden samt aggressionshandlinger).

[68] ECHR's artikel 13 forpligter medlemsstater til at sikre, at "enhver, hvis rettigheder og frihed (…) krænkes, skal have et effektivt retsmiddel foran en national myndighed". Dette skal ikke nødvendigvis være en retsmyndighed, som ECtHR har klarlagt i Klass §56 og 67.

[69] Klass § 56 og 67.

[70] ECtHR, Klass § 21 og 53.

[71] G 10-Kommissionen (på tidspunktet for dommen) består af tre medlemmer, hvoraf formanden skal være kvalificeret til at beklæde et retsembede, Klass § 21 og 53).

[72] ECtHR, Kennedy § 167; Klass § 21 og 53.

hjælp fra andre bureauer, og endelig dens bemyndigelse til at afhjælpe manglende overholdelse.

3.5.3.4 Ombudspersonsmekanismens anvendelsesområde

Hvad angår adgang til ombudspersonsmekanismen mener WP29, at alle personer, som er underlagt EU-lovgivning, skal være dækket af sikkerhedsforanstaltningerne under værnet om privatlivets fred. Det vil ikke være acceptabelt at gøre en forskel baseret på nationalitet, især i lyset af at de grundlæggende rettigheder i EU gælder for alle og ikke kun for dem, der har et europæisk pas. Bilag III henviser til en "fysisk person i EU" uden yderligere at definere, hvem det er. Arbejdsgruppen beklager denne uvished og foreslår, at der fremsættes en afklaring i den forstand, at alle personer, som er underlagt EU-lovgivning, har ret til få sin anmodning til ombudspersonen behandlet i henhold til memorandummets betingelser. Kommissionen og USA skal endvidere anføre spørgsmålet vedrørende, i hvilken udstrækning værnet om privatlivets fred også vil gælde for borgere/bosiddende i landene i EØS og Schweiz, som tidligere var dækket af Safe Harbor-ordningen.

Desuden anfører WP29 nogen uvished, hvad angår ombudspersonsmekanismens anvendelsesområdet. Hvor memorandummet fremsætter, at ombudspersonen gives ansvaret for at behandle anmodninger vedrørende national sikkerhed i forbindelse med data, der videregives fra EU til USA i henhold til alle videregivelsesværktøjer, som er tilgængelige under EU-lovgivning, gøres det ligeledes klart, at den fremsætter en mekanisme "vedrørende signalefterretning". Sidstnævnte begreb antyder kun, at sådanne dataoverførsler er dækket, hvor dataene blev indsamlet ved hjælp af signalefterretning, hvilket fører til spørgsmålet, om data indsamlet under FISA, f.eks. anses som "signalefterretning". Det lader til at være tilfældet i sagen, hvad angår afsnit 702 som forklaret i fremstillingen fra ODNI, punkt 10[73]. WP29 beklager imidlertid, at anvendelsen af begrebet "signalefterretning" skaber unødvendig uvished i denne kontekst.

Endnu en konsekvens er, at det er arbejdsgruppens opfattelse, at ombudspersonens mekanisme ikke dækker anmodninger vedrørende retshåndhævelsesbureauers aktindsigt[74]. Hvis det er tilfældet, ville det forblive uklart, om anmodninger fra nogle bureauer, navnligt CIA, ville være dækket af mekanismen.

3.5.3.5 "Søgsmålskompetence" og anmodningsproceduren

Det er meget vanskeligt at anlægge sag mod den amerikanske regerings overvågningsmetoder i ordinære domstole i USA. Arbejdsgruppen er bekendt med, at højesteretten har afvist søgsmålskompetence i efterretningssager, hvor ansøgeren ikke var i stand til at vise individuel "konkret, partikulariseret samt faktisk eller overhængende skade"[75]. I denne henseende er etableringen af ombudspersonen et vigtigt skridt, da det tilvejebringer en vej til en form for retslig afhjælpning, som ellers ikke ville eksistere. Derfor tager arbejdsgruppen imod

[73] Værnet om privatlivets fred, bilag VI, punkt 10.
[74] Memorandum om etableringen af en ombudsperson, punkt 1.
[75] Clapper mod Amnesty International USA, 568 U.S. ___ (2013) II. punkt 10.

afklaringen i afsnit 3, stk. c. Baseret på dette afsnit er der ikke behov for at påvise, at anmoderens data rent faktisk er blevet tilgået gennem signalefterretningsaktiviteter for at indsende en anmodning i henhold til den nye mekanisme.

Arbejdsgruppen godkender i det store og hele proceduren til identifikation af sagsøgeren i henhold til ombudspersonsmekanismen. Det giver virkelig mening, at identifikationen finder sted på europæisk område, da det også er tilfældet for adgangsmekanismen i henhold EU's og USA's TFTP2-aftale. Arbejdsgruppen formår imidlertid ikke at forstå, hvorfor verificeringen i EU skal udføres af "medlemsstatsinstanserne, som er kvalificerede til at føre tilsyn med nationale sikkerhedstjenester". I første omgang forekommer det usandsynligt, at Europa-Kommissionen efter artikel 4, stk. 2, i traktaten om Den Europæiske Union vil være i stand til at tildele opgaver til disse instanser, som tydeligt falder inden for medlemsstaternes kompetence.

I lyset af de forskellige tilsynsmekanismer for nationale sikkerhedstjenester i medlemsstater kan de tilsvarende myndigheders indblanding imidlertid påvirke systemets effektivitet i alvorlig grad for statsborgere i medlemsstaterne. For eksempel i sager, hvor der er flere myndigheder, der er ansvarlige for tilsynet med de nationale sikkerhedstjenester, og det kan være vanskeligt for den fysiske person at identificere den relevante tjeneste, hvor gældende nationale retsregler ikke tager højde for den mulighed, at fysiske personer kan komme i kontakt med den relevante tilsynsførende instans, eller hvor disse myndigheder ikke er etableret på en sådan måde, at de egner sig til at udføre de opgaver, som de pålægges i udkastet til tilstrækkelighedsafgørelsen[76]. Når der tages højde for databeskyttelsesmyndigheder indblanding i anvendelsen af og tilsynet med værnet om privatlivets fred, samt deres tilsvarende rolle ifølge TFTP2-aftalen, giver det mere mening at tildele denne opgave til nationale myndigheder for databeskyttelse i medlemsstaterne. Arbejdsgruppen understreger, at den anser det for usandsynligt, at klassificerede oplysninger vil blive behandlet som del af en procedure foran ombudspersonen til værnet om privatlivets fred, da et svar kun ville være "i overensstemmelse eller ikke i overensstemmelse, men afhjulpet".

3.5.3.6 Uafhængighed

Den amerikanske justitsministers fremstillinger gør det klart, at ombudspersonens stilling vil blive udført af en understatssekretær for det amerikanske udenrigsministerium. Han indstilles af præsidenten og kræver bekræftelse fra senatet. Ombudspersonens rolle kræver ikke yderligere bekræftelse; tildelingen af ombudspersonens rolle er tilstrækkelig. Understatssekretæren indstilles af den amerikanske præsident, vejledt af udenrigsministeren som ombudspersonen og bekræftet af det amerikanske senat i hendes rolle som understatssekretær. Som fremstillingerne i brevet og memorandummet understreger, er ombudspersonen "uafhængig fra det amerikanske efterretningsfællesskab". WP29 stiller imidlertid spørgsmålstegn ved, om ombudspersonen er oprettet inden for det mest egnede ministerium. Der lader til at være behov for noget kendskab og forståelse af

[76] For eksempel kan fysiske personer, i nogle af EU's medlemsstater, kun få indsigt i oplysninger, som opbevares af de nationale sikkerhedstjenester via en anmodning til Landsretten.

efterretningsfællesskabets virkemåde for effektivt at udføre ombudspersonens rolle, mens der samtidig rent faktisk er behov for tilstrækkelig afstand fra efterretningsfællesskabet for at kunne handle uafhængigt.

Værnet om privatlivets fred opretter ikke specifikke kriterier for afskedigelsen af ombudspersonen. Det er således arbejdsgruppens opfattelse, at ombudspersonen kan afskediges i sin rolle som ombudsperson på samme måde, som han kan afskediges i sin rolle som understatssekretær i udenrigsministeriet, hvilket potentielt kan underminere ombudspersonens uafhængige position.

Udpegningen af en understatssekretær i udenrigsministeriet som en ombudsperson er tydeligvist anderledes, hvad angår uafhængigheden fra den ordinære domstols klarlæggende jurisdiktion for en fysisk persons retslige afhjælpning. Spørgsmålet er således, om ombudspersonen, hvad angår uafhængighed, kan anses som værende på lige fod med andre uafhængige tilsynsinstanser, som er blevet konstateret at være overensstemmende. I denne overvågningskontekst vil disse navnligt være Investigatory Powers Tribunal (IPT) i Storbritannien og G10-Kommissionen i Tyskland.

Om det er tilfældet skal vurderes yderligere ved at analysere de beføjelser, der er tildelt den "uafhængige".

3.5.3.7 Undersøgelsesbeføjelser

I Kadi II-sagen afsagde EU-Domstolen kendelse, hvad angår charterets artikel 47, om, at "den pågældende person skal være i stand til at fastslå begrundelserne, hvorpå beslutningen om ham er baseret, enten ved at overveje selve beslutningen eller ved at anmode om eller opnå offentliggørelse af disse grunde, uden præjudice til beføjelsen for den domstol, der har jurisdiktion til at pålægge den pågældende myndighed at offentliggøre de oplysninger, for at gøre det muligt for ham at forsvare sine rettigheder under de bedst mulige forhold"[77]. Domstolene i Den Europæiske Union skal sikre, at beslutningen tages på et tilstrækkeligt solidt og sagligt grundlag[78]. Den fremsætter tydeligt, at "hemmeligheden eller fortroligheden ved […] oplysninger eller dokumentationsmateriale ikke er en gyldig protest", i det mindste ikke i domstolene i Den Europæiske Union[79]. Derfor konkluderer arbejdsgruppen, at ombudspersonen skal have oplysninger og dokumentationsmateriale, der understøtter de begrundelser, som er nødvendige til at udføre en foranstaltning, for at opfylde EU-Domstolens krav[80].

Det er stadig uklart, hvilket omfang ombudspersonens undersøgelsesbeføjelser vil have. Både Kommissionens udkast til afgørelse og bilag III fra udenrigsministeriet er ikke ret tydeligt i denne henseende. Så vidt arbejdsgruppen forstår, skal ombudspersonen have tilstrækkelige oplysninger for at være i stand til at anføre, om en sikkerhedstjenestes databehandling finder

[77] Kadi II §100.
[78] Kadi II § 119.
[79] Kadi II § 125.
[80] Kadi II §122; selvom den pågældende myndighed ikke skal frembringe alle oplysninger og dokumentationsmateriale, som danner basis for en foranstaltning.

sted i overensstemmelse med loven, og hvis ikke, sørge for, at den ikke-overensstemmende situation afhjælpes. Hverken brevet fra udenrigsministeriet eller Kommissionens udkast til afgørelse angiver imidlertid, om ombudspersonen vil have direkte indsigt i de data, der opbevares om den pågældende fysiske person, og således kan udføre sin egen undersøgelse, eller om han/hun kun kan støtte sig til rapporter fra andre amerikanske embedsmænd.

3.5.3.8 Afhjælpende beføjelser

Det forbliver temmelig uklart i lyset af memorandummet, på hvilken måde ombudspersonen kan sørge for afhjælpning af manglende overholdelse. I kombination med manglende klarhed vedrørende undersøgelsesbeføjelserne forbliver det desuden uklart, i hvilket omfang ombudspersonen som sådan vil være effektivt i stand til at sørge for afhjælpning af manglende overholdelse, og hvad resultatet af en sådan udøvelse ville være. Kunne det betyde, at data, som blev skaffet på en ikke-overensstemmende måde (dvs. ulovligt), ikke længere kan anvendes i nogen procedure og skal slettes?

Det er endvidere arbejdsgruppens opfattelse, at værnet om privatlivets fred ikke tager højde for en ankesag mod eller evaluering af "afgørelsen" fra ombudspersonens side.

Til sidst, hvad angår ombudspersonens kommunikation med sagsøgeren efter hendes undersøgelse af en klage, må ombudspersonen ikke afsløre, om efterretningsfællesskabet har udvist nogen ulovlig adfærd. Det fremsatte svar vil altid være det samme, og det vil være uspecifikt. I Kadi II-sagen afsagde EU-Domstolen kendelsen om, at den kompetente myndighed (som en tilsynsførende instans) er forpligtet til at fremsætte årsager, der nødvendiggør alle omstændigheder, selvom TFEU's artikel 296 ikke kræver et detaljeret svar[81].

3.5.4 Konklusion

Eksistensen af effektive retsmidler til fysiske personer er fortsat en bekymring for WP29. For det første giver udkastet til tilstrækkelighedsafgørelsen ikke et klart svar på spørgsmålet om, i hvilke situationer og under hvilke forudsætninger fysiske personer kan anlægge en sag for at fastslå deres rettigheder.

WP29 anerkender og byder indførelsen af en alternativ afhjælpningsmekanisme i form af ombudspersonen velkommen, hvilket er en unik udvikling i relationerne mellem EU og et tredjeland. Bortset fra behovet for at afklare begrebet "fysiske personer i EU" som nævnt tidligere giver mekanismen dem endnu en middel til at søge afhjælpning fra den amerikanske regering for at sikre, at alle ansøgerens persondata bliver behandlet i overensstemmelse med amerikansk lov.

Samtidig bemærker WP29 som led i sin vurdering af ombudspersonsmekanismen i forhold til standarderne for et uafhængigt nævn i den betydning, som er fremsat i artikel 47 i charteret, og de krav, som EU-Domstolen og ECtHR har fastsat i deres retslære for overvågningssager,

[81] Kadi II § 116.

at der er væsentlige mangler. For det første er der bekymringer, om ombudspersonen kan betragtes (formelt og fuldt ud) som værende uafhængig, især i lyset af hvor relativt nemt det er at afskedige politisk udnævnte personer. For det andet er der stadig bekymringer vedrørende ombudspersonens bemyndigelse til at udøve effektiv og vedvarende kontrol. Baseret på de tilgængelige oplysninger i bilag III kan WP29 ikke drage den konklusion, at ombudspersonen hele tiden vil have direkte indsigt i alle oplysninger, filer og IT-systemer, der er nødvendige for, at han kan foretage sin egen evaluering, og heller ikke at han virkelig tvinger de ansvarlige efterretningsbureauer til at standse al databehandling, som ikke overholder betingelserne, navnlig i tilfælde af uenighed vedrørende spørgsmålet, om databehandlingen overholder loven eller ej. Yderligere afklaring af ombudspersonens position og bemyndigelse kan muligvis fjerne WP29's bekymringer.

3.6 Konkluderende bemærkninger om sikkerhedsforanstaltninger og begrænsninger, der er relevante for amerikanske myndigheder for national sikkerhed

WP29 roser for det første Kommissionen og de amerikanske myndigheder for hele den indsats, der er gjort for at øge gennemsigtigheden af den indvirkning, som amerikanske overvågningsprogrammer kan have på data, der videregives under værnet om privatlivets fred – eller ethvert andet videregivelsesværktøj for den sags skyld. Der er truffet væsentlige foranstaltninger siden de første Snowden-afsløringer i juni 2013. Ikke desto mindre bemærker WP29, at der stadig er bekymringer. Som absolut minimum er der behov for yderligere forklaring og afklaring for så vidt angår rettighederne og forpligtelserne under værnet om privatlivets fred.

WP29's to største bekymringer er, at de amerikanske myndigheder ikke helt udelukker enorm og vilkårlig dataindsamling, og at ombudspersonens bemyndigelse og position ikke er blevet fremsat mere detaljeret. Desuden skal de nationale databeskyttelsesmyndigheder være kompetente til at starte en procedure over for ombudspersonen på vegne af en fysisk person fremfor de tilsynsførende instanser for efterretningsbureauerne. Selvom WP29 helt sikkert anerkender forsøgene på at imødekomme de bekymringer, som databeskyttelsesmyndighederne har rejst, vil yderligere sikkerhedsforanstaltninger blive hilst velkomne for at sikre, at alle indgreb, der kan skyldes de amerikanske overvågningssystemer, er nødvendige i et demokratisk samfund.

4. VURDERING AF RETSHÅNDHÆVELSENS GARANTIER FOR VÆRNET OM PRIVATLIVETS FRED

4.1 Introduktion

Hvad angår offentlig aktindsigt til retshåndhævelsesformål, anfører WP29, at principperne om privatlivets fred i bilag II til værnet om privatlivets fred indeholder en undtagelsesbestemmelse, der er identisk med den undtagelsesbestemmelse, der blev fastlagt i principperne om Safe Harbour. Undtagelsesbestemmelsens almene natur er derfor opretholdt, hvilket betyder, at de nye principper om privatlivets fred muliggør indgreb i de personers grundlæggende rettigheder, hvis persondata videregives fra EU til USA "på grundlag af

kravene vedrørende statens sikkerhed og almenvellet eller på grundlag af den nationale amerikanske lovgivning"[82].

Et af de primære kritikpunkter, som domstolen havde i forbindelse med Safe Harbour-afgørelsen i Schrems-sagen var imidlertid, at den ikke indeholder nogen "konstateringer om, hvorvidt der i USA foreligger regler af statslig karakter, hvorved det tilsigtes at begrænse de eventuelle indgreb i de grundlæggende rettigheder hos de personer, hvis oplysninger bliver videregivet fra Unionen til USA".

Derfor anerkender WP29 indsatsen fra den amerikanske regering om at komme med mere indsigt i de retslige rammer vedrørende indgrebet i persondata, der er videregivet under værnet om privatlivets fred til retshåndhævelsesformål, inklusive de relevante begrænsninger og sikkerhedsforanstaltninger. Samtidig understreger WP29, at den tager spørgsmålet om offentlig aktindsigt i betragtning, idet den minder om, at ethvert indgreb i de grundlæggende rettigheder for privatlivets fred og databeskyttelse skal kunne forsvares i et demokratisk samfund. Derfor har WP29 analyseret retshåndhævelsens garantier for værnet om privatlivets fred ved hjælp af de rammer, som er fremsat i afsnit 1.2 i denne udtalelse.

4.2 Anvendelse af de europæiske essentielle garantier, så retshåndhævelsesmyndigheder kan tilgå data, der opbevares af virksomheder

4.2.1 Retshåndhævelsesmyndigheders aktindsigt skal være i overensstemmelse med loven og baseret på klare, præcise og forståelige regler

Bilag VII til værnet om privatlivets fred indeholder et brev fra det amerikanske justitsministerium, der "giver en kort oversigt over de primære undersøgelsesværktøjer, som anvendes til at få kommercielle data og andre fortegnelsesoplysninger fra virksomheder i USA til strafferetlige håndhævelsesformål eller formål vedrørende den offentlige interesse (civilretlig og regulatorisk), inklusive de adgangsbegrænsninger, der er fremsat i disse myndigheder".

Alle procedurer, der er nævnt i bilag VII, stammer enten direkte fra den amerikanske forfatning (den fjerde forfatningsændring), fra positiv og procesret eller fra justitsministeriets retningslinjer og politikker. Bilag VII henviser imidlertid ikke specifikt til alle vedtægter, der fremsætter disse procedurer, men fokuserer i stedet på en kort beskrivelse af selve procedurerne. Bilag VII nævner også, at "der er andre retslige grundlag for virksomheder til at bestride dataanmodninger fra administrative bureauer baseret på deres specifikke industrier og de typer data, de behandler", ved at komme med ikke-udtømmende eksempler såsom loven om bankhemmeligholdelse, loven om retfærdig kreditrapportering, loven om retten til økonomisk privatliv.

WP29 anfører, at rammerne for vedtægter, procedurer og politikker er fragmenteret, og at det relevante retslige grundlag til en givet anmodning om aktindsigt vil afhænge af de søgte datas natur, virksomhedens natur, de retslige procedurers natur (strafferetlig, administrativ,

[82] Schrems, § 87.

vedrørende anden offentlig interesse) samt beskaffenheden af den enhed, som anmoder om aktindsigt.

Da alle gældende regler om retshåndhævelsesmyndigheders begrænsning af aktindsigt, der videregives under værnet om privatlivets fred, er baseret på forfatningen, på positiv ret og på justitsministeriets åbne politikker, har WP29 taget højde for disse reglers formodede tilgængelighed. Reglernes klarhed og præcision kan imidlertid kun vurderes i hver enkelt type procedure og anmodning om aktindsigt. Derfor beklager WP29 at måtte anføre, at ud fra de tilgængelige data i bilag VII til værnet om privatlivets fred og konklusionerne i udkastet til afgørelsen kan en sådan vurdering ikke foretages i øjeblikket.

4.2.2 Nødvendighed og proportionalitet i forbindelse med de lovlige mål, der tilstræbes, skal vises

WP29 tager til efterretning, at anmodning om data til retshåndhævelsesformål kan overvejes til at følge et lovligt formål. For eksempel accepterer artikel 8, stk. 2, i ECHR indgreb i retten til beskyttelse af privatlivet fra en offentlig myndighed "i (…) den offentlige sikkerheds interesse, (…) for at forhindre uorden eller kriminalitet". Sådanne indgreb er imidlertid kun acceptable, når de er nødvendige og proportionale[83].

I henhold til EU-Domstolens udarbejdede retspraksis kræver princippet om proportionalitet, at de lovgivende retsmidler, der foreslår indgreb i retten til privatliv og til beskyttelsen af persondata, "er relevante for at nå de lovlige mål, som tilstræbes af *lovgivningen, som er til debat,* og ikke overskrider grænserne for, hvad der er relevant og nødvendigt for at nå disse mål"[84] (vores emfase). Derfor foretages vurderingen af nødvendighed og proportionalitet altid i forbindelse med et bestemt retsmiddel forudset af lovgivningen.

De amerikanske myndigheder angiver i bilag VII, at føderale anklagere og føderale efterforskere skal være i stand til at få aktindsigt i dokumenter og andre fortegnelsesoplysninger fra organisationer via "flere slags obligatoriske retsprocesser, inklusive stævninger fra anklagejuryer, administrative stævninger og ransagningskendelser" og kan få fat i anden kommunikation "i henhold til føderale, strafferetlige telefonaflytninger og myndigheder, der logger udgående opkald"[85]. Desuden kan bureauer med civilretlige og regulatoriske ansvar udstede stævninger til organisationer for "forretningsfortegnelser, elektronisk opbevarede oplysninger eller andre materielle elementer"[86]. Bilag VII angiver endvidere, at disse retsprocesser generelt anvendes til at få oplysninger fra "virksomheder" i USA, uanset om de er certificerede eller ikke falder inden for rammerne for værnet om privatlivets fred og "uden hensyn til den registreredes nationalitet". Med andre ord lader det til, at genstande for disse beskyttelser er virksomhederne og ikke selve de fysiske personer.

[83] Se arbejdsdokumentet om de europæiske essentielle garantier, punkt 7-9. For en generel vurdering af begreberne nødvendighed og proportionalitet henvises der til WP29 "Udtalelse 01/2014 om anvendelsen af begreberne nødvendighed og proportionalitet samt databeskyttelse inden for retshåndhævelsessektoren", 27. februar 2014.
[84] Digitale rettigheder Irland, §46, og retspraksis anført deri.
[85] Bilag VII, punkt 2.
[86] Bilag VII, punkt 4.

Foruden bilag VII indeholder udkastet til afgørelsen – som er baseret på principperne om privatlivets fred – Kommissionens konklusioner om eksistensen, i USA, af regler til begrænsning af indgreb i de personers grundlæggende rettigheder, hvis persondata videregives fra EU til USA under værnet om privatlivets fred.

Især henviser konklusionerne i udkastet til afgørelsen til relevante begrænsninger og sikkerhedsforanstaltninger under den fjerde forfatningsændring i den amerikanske forfatning, og i henhold til disse kræver gennemsøgninger og beslaglæggelser fra retshåndhævelsesmyndigheder principielt en dommerkendelse, når der er vist bestyrket mistanke[87]. Konklusionerne henviser også til det faktum, at undtagelsestilfældene, hvor kravet om en dommerkendelse ikke er gældende, er retshåndhævelsen underlagt en rimelighedstest[88].

Ikke desto mindre gør konklusionerne det ikke klart, hvordan disse sikkerhedsforanstaltninger gælder for ikke-amerikanske personer. Faktisk anerkender udkastet til afgørelsen i en sagsfremstilling, at "beskyttelsen under den fjerde forfatningsændring ikke strækker sig til ikke-amerikanske personer, som ikke er bosiddende i USA"[89]. Det fremsættes endvidere i de samme afsnit i udkastet til afgørelsen, at ikke-amerikanske personer" drager indirekte fordel gennem den beskyttelse, der ydes til amerikanske virksomheder, som bevarer de persondata, og som er modtagerne af retshåndhævelsesanmodningerne". WP29 beklager imidlertid at måtte anføre, at denne konklusion ikke kommer med nogen henvisning til en retslig kilde, hverken i positiv ret eller retspraksis.

I det hele taget anfører WP29, at systemet med undersøgelsesværktøjer anvendes til at få fat i kommercielle data og andre fortegnelsesoplysninger fra virksomheder i USA til formål for strafferetlig håndhævelse eller offentlig interesse – inklusive adgangsbegrænsninger og sikkerhedsforanstaltninger – er et komplekst sikkerhedsforanstaltningsmiljø. Ud fra tilgængelige oplysninger kan dette system ikke vurderes generelt i øjeblikket. Specifikke vurderinger i individuelle tilfælde er nødvendige for en virkelig vurdering af nødvendigheden og proportionaliteten ved retshåndhævende undersøgelsesforanstaltninger i forbindelse med de grundlæggende rettigheder til privatliv og databeskyttelse.

4.2.3 Der skal være en uafhængig tilsynsmekanisme

WP29 tager til efterretning, at det faktum, at de fleste procedurer, der er beskrevet i bilag VII, forudsætter indblandingen fra en domstols afgørelse, før myndighederne får aktindsigt (f.eks. domkendelser til at logge udgående opkald og telefonaflytninger, domkendelser til overvågning i henhold til den føderale lov om telefonaflytning, ransagningskendelser – regel 41). Det lader imidlertid ikke til, at de alle kræver a priori indblanding fra en domstol. For eksempel kan civilretlige og regulatoriske myndigheder "udstede stævninger"[90]. I disse

[87] Udkast til tilstrækkelighedsafgørelsen, § 107.
[88] Værnet om privatlivets fred, § 107.
[89] Udkast til tilstrækkelighedsafgørelsen, § 108.
[90] Bilag VII, punkt 4.

tilfælde er der mulighed for en ex post retslig kontrol med stævningens rimelighed, som "en modtager af en administrativ stævning kan bestride håndhævelsen af den stævning i retten"[91].

Ud fra de tilgængelige oplysninger anfører WP29, at - hvad angår retshåndhævelsesmyndigheders aktindsigt, der opbevares af virksomheder i USA lader der til at være en rimelig robust, uafhængig tilsynsmekanisme på plads.

4.2.4 Effektive retsmidler skal være tilgængelige for den fysiske person

Som tidligere nævnt "strækker beskyttelsen under den fjerde forfatningsændring sig ikke til ikke-amerikanske personer, som ikke er bosiddende i USA"[92]. Det betyder, at en ikke-amerikansk person ikke vil kunne bestride dommerkendelser eller stævninger i domstolen ved at påberåbe sig den fjerde forfatningsændring. Udkastet til tilstrækkelighedsafgørelsen fremsætter, at ikke-amerikanske personer drager indirekte fordel gennem den beskyttelse, der ydes til amerikanske virksomheder, som bevarer de persondata, og som er modtagerne af retshåndhævelsesanmodningerne. WP29 anfører imidlertid, at selvom denne beskyttelse ville være effektiv, betyder det ikke, at effektive retsmidler er tilgængelige for fysiske personer, da genstanden for retten til et effektivt retsmiddel i dette scenarie lader til at være virksomheden, som modtager anmodningen om aktindsigt, og ikke den fysiske person, hvis data er til debat.

Bilag VII indeholder ikke nogen yderligere oplysninger, hvad angår mulige retsmidler, der stammer fra positiv ret, og som er tilgængelig for ikke-amerikanske personer, når myndigheder eller virksomheder på ulovlig vis giver eller får indsigt i indholdet af deres data.

WP29 glæder sig over, at den nyligt vedtagne Judicial Redress Act[93] giver adgang til retsmidler for ikke-amerikanske personer. Disse rettigheder er imidlertid begrænset til tydeligt definerede handlingsforløb: Retten til at få rettelse og aktindsigt og advokatsalærer, når et "udpeget føderalt bureau eller komponent" afviser ændring af data eller afviser indsigt i sådanne data, samt retten til at få civilretlige retsmidler i tilfælde af "bevidste eller forsætlige" offentliggørelser af data.

Den amerikanske retspraksis, som der henvises til i fodnoterne til de relevante sagsfremstillinger i udkastet til afgørelsen, særligt byen Ontario mod Quon[94], Maryland mod King[95] og Samson mod Californien[96], er heller ikke relevante for at vurdere, om ikke-amerikanske personer kan fremsætte et krav for retten for at bestride retmæssigheden ved et indgreb i deres privatlivs fred[97]. Alle sager henviser til amerikanske personers ret til privatliv,

[91] Bilag VII, punkt 4.
[92] Udkastet til tilstrækkelighedsafgørelsen, §108.
[93] Loven om retslig afhjælpning af 2015, H.R. 1428.
[94] *Byen Ontario, Cal. mod Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland mod King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson mod Californien*, 547 U.S. 843, 848 (2006).
[97] I *Ontario mod Quon* fastholdt retten, at byen Ontario ikke krænkede sine medarbejderes rettigheder til den fjerde forfatningsændring, eftersom byens indsigt i indholdet i den pågældende medarbejders private meddelelser var rimelig, da den var motiveret af et lovligt arbejdsrelateret formål og ikke overdrev anvendelsesområdet. I *Samson mod Californien* konstaterede retten, at "den fjerde forfatningsændring ikke forhindrer en politibetjent i udføre en kropsvisitation af en prøveløsladt person uden involveret mistanke". I *Maryland mod King* fastholdt retten, at når betjente foretager en anholdelse underbygget af begrundet mistanke for at tilbageholde en mistænkt for en alvorlig forbrydelse og bringe ham til stationen til

og de indeholder alle afgørelser fra den amerikanske højesteret, der rent faktisk begrænser gyldigheden af den fjerde forfatningsændring.

I det hele taget anerkender og bifalder WP29 vedtagelsen af loven om retslig afhjælpning, men den forbliver i tvivl, om effektive retsmidler rent faktisk er tilgængelige for individuelle registrerede.

4.3 Afsluttende bemærkninger

WP29 bifalder og anerkender indsatsen fra den amerikanske regering om at komme med mere indsigt i den retslige ramme vedrørende indgrebet i persondata, der er videregivet under værnet om privatlivets fred til retshåndhævelsesformål, inklusive de relevante begrænsninger og sikkerhedsforanstaltninger.

WP29 anfører, at retshåndhævelsesmyndighedernes system med undersøgelsesværktøjer, inklusive de gældende begrænsninger og sikkerhedsforanstaltninger, er både omfattende og komplekse, og at oplysningerne indeholdt i værnet om privatlivets fred er kortfattet. Derfor beklager WP29, at den ud fra de begrænsede oplysninger (dvs. i bilag VII til værnet om privatlivets fred og om konklusionerne i udkastet til afgørelsen) ikke er i stand til på nuværende tidspunkt at komme med en omfattende vurdering af de gældende reglers tilgængelighed, adækvans, nødvendighed og proportionalitet. Til trods for WP29's andre konklusioner vedrørende værnet om privatlivets fred i denne udtalelse vil en sådan vurdering muligvis være en del af en årlig vurdering af værnet om privatlivets fred.

Hvad angår retshåndhævende myndigheders aktindsigt, anfører WP29, at der lader til at være indført en rimelig robust, uafhængig tilsynsmekanisme. Endvidere bifalder WP29 vedtagelsen af loven om retslig prøvelse, som giver ikke-amerikanske personer retten til retslig prøvelse. WP29 anfører imidlertid, at disse rettigheder er begrænsede. Foruden konklusionen om, at en ikke-amerikansk person ikke vil kunne bestride arrestordrer eller stævninger i retten, der gør den fjerde forfatningsændring gældende, er der fortsat bekymringer om, hvorvidt den enkelte registrerede rent faktisk har adgang til effektive retsmidler på retshåndhævelsesområdet.

5. KONKLUSIONER OG ANBEFALINGER

WP29 bifalder for det første den kendsgerning, at der inden for fem måneder efter ugyldiggørelsen af Safe Harbour-principperne blev fremlagt et nyt udkast til en tilstrækkelighedsafgørelse, der indeholdt mange forbedringer sammenlignet med den tidligere mekanisme. Arbejdsgruppen er især tilfreds med den øgede gennemsigtighed, der tilbydes med indførslen af to lister for værnet om privatlivets fred på det amerikanske handelsministeriums websted: én liste, der indeholder fortegnelser over de organisationer, der overholder værnet om privatlivets fred, og én liste, der indeholder fortegnelserne over de organisationer, der tidligere har overholdt værnet, men ikke længere gør det. Den øgede gennemsigtighed vedrørende den offentlige adgang til oplysninger, der videregives under

varetægtsfængsling, er det at tage og analysere en spytprøve fra den anholdtes DNA, ligesom fingeraftryk og fotografering, en lovlig politiregistreringsprocedure, som er rimelig i henhold til den fjerde forfatningsændring.

værnet om privatlivets fred, enten til formål for den nationale sikkerhed eller retshåndhævelse, bifaldes også. Endelig er WP29 også meget tilfreds med at kunne konstatere, at alle dataoverførsler til USA fremover vil have samme beskyttelse: Der findes ingen specifikke retsbestemmelser, der foretrækker ét værktøj fremfor et andet.

5.1 Tre bekymringspunkter

Der er imidlertid fortsat tre vigtige bekymringspunkter, som efter WP29's mening vil skulle behandles.

Den første bekymring er, at den ordlyd, som anvendes i udkastet til tilstrækkelighedsafgørelsen, ikke tvinger organisationer til at slette data, hvis de ikke længere er nødvendige. Dette er et afgørende element i EU's databeskyttelseslovgivning for at sikre, at dataene ikke bevares længere end nødvendigt for at nå det formål, hvortil dataene blev indsamlet. For det andet forstår WP29 ud fra bilag VI, at den amerikanske regering ikke helt udelukker den fortsatte indsamling af enorme og vilkårlige data. WP29 har hele tiden fastholdt, at sådan dataindsamling er et ubegrundet indgreb i fysiske personers grundlæggende rettigheder. Det tredje bekymringspunkt vedrører indførelsen af ombudspersonsmekanismen. Skønt WP29 bifalder dette hidtil usete trin, der skaber endnu en afhjælpnings- og tilsynsmekanisme for fysiske personer, er der fortsat bekymringer om, hvorvidt ombudspersonen har tilstrækkelig bemyndigelse til at fungere effektivt. Som minimum skal både ombudspersonens bemyndigelse og position afklares for at vise, at rollen er helt uafhængig og kan tilbyde et effektivt retsmiddel til databehandling, som ikke overholder reglerne.

5.2 Anbefalede afklaringer

Udover de punkter, der er nævnt ovenfor, har WP29 gennem hele denne udtalelse angivet forskellige punkter, hvor yderligere afklaring af tilstrækkelighedsafgørelsen vil være en god idé. Vigtigst af alt vedrører dette behovet for at sikre, at de nøglebegreber vedrørende databeskyttelse, der anvendes i værnet om privatlivets fred, er defineret og anvendes på en konsekvent måde, hvilket ikke er tilfældet i øjeblikket. Indførelsen af en ordliste under ofte stillede spørgsmål til værnet om privatlivets fred med definitioner, som EU og USA ideelt er blevet enige om, ville være en god idé. WP29 konkluderer også, at der ikke findes tilstrækkelige rammer for videregivelse af persondata fra EU, særligt hvad angår deres anvendelsesområde, begrænsningen af deres formål og de garantier, der gælder for videregivelser til agenter. Hvad angår retshåndhævende myndigheders adgang til oplysninger under værnet om privatlivets fred, især vedrørende lovgivningens adækvans, er det en bekymring som følge af det amerikanske retsvæsens omfattende og komplekse natur på både føderalt niveau og delstatsniveau, og de begrænsede oplysninger, der indgår i tilstrækkelighedsafgørelsen.

Værnet om privatlivets fred er den første tilstrækkelighedsafgørelse, der er blevet lavet udkast til, siden teksterne under GDPR blev aftalt i princippet. Og alligevel er mange af de databeskyttelsesmæssige forbedringer, som tilbydes fysiske personer, ikke afspejlet i værnet

om privatlivets fred. WP29 anbefaler derfor, at der kort efter GDPR's ikrafttrædelse foretages en evaluering af denne tilstrækkelighedsafgørelse samt af de tilstrækkelighedsafgørelser, som sendes til tredjelande.

En endelig anbefaling, som WP29 gerne vil fremhæve her, vedrører den fælles evaluering. WP29 bifalder den kendsgerning, at tilstrækkelighedsafgørelsen under værnet om privatlivets fred vil blive evalueret årligt med stor inddragelse af databeskyttelsesmyndigheder og andre relevante parter. Den ser gerne, at alle parter i god tid inden den første evaluering bliver enige om elementerne i de fælles evalueringer, inklusive udkastet til og præsentationen af evalueringsrapporten.