ARTIKEL 29-ARBETSGRUPPEN FÖR UPPGIFTSSKYDD

**16/SV**
**WP 238**

# Yttrande 01/2016 om förslaget till beslut om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna

**Antaget den 13 april 2016**

Denna arbetsgrupp inrättades genom artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ för uppgiftsskydd och integritetsskydd. Arbetsuppgifterna finns beskrivna i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

För sekretariatet svarar direktorat C (Grundläggande rättigheter och unionsmedborgarskap) vid Europeiska kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor, B-1049 Bryssel, Belgien, Kontor MO-59 02/013.

Webbplats: http://ec.europa.eu/justice/data-protection/index_sv.htm

## SAMMANFATTNING

Den 29 februari 2016 offentliggjorde kommissionen ett meddelande, ett förslag till beslut om adekvat skyddsnivå och de bilagor som ska bilda ett nytt regelverk för transatlantiskt utbyte av personuppgifter för kommersiella ändamål: skölden för skydd av privatlivet i EU och Förenta staterna (nedan kallad *skölden för skydd av privatlivet*) som ska ersätta det beslut om safe harbour-principerna som Europeiska unionens domstol (*nedan kallad EU-domstolen*) ogiltigförklarade den 6 oktober 2015 i Schremsmålet.

Artikel 29-arbetsgruppen (nedan kallad *arbetsgruppen*) har bedömt dessa handlingar i enlighet med artikel 30.1 c i direktiv 95/46/EG för att yttra sig om förslaget till beslut om adekvat skyddsnivå. Arbetsgruppen bedömde både de kommersiella aspekterna och de möjliga undantagen från principerna om skölden för skydd av privatlivet för ändamål som berör nationell säkerhet, brottsbekämpning och allmänhetens intresse.

Arbetsgruppen tog hänsyn till den gällande EU-lagstiftningen om skydd av personuppgifter i enlighet med direktiv 95/46/EG och de grundläggande rättigheterna till respekt för privatlivet och skydd av personuppgifter i enlighet med artikel 8 i Europeiska konventionen om mänskliga rättigheter och artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Den tog också hänsyn till den rätt till ett effektivt rättsmedel och till en opartisk domstol som fastställs i artikel 47 i stadgan, samt rättspraxis i fråga om de olika grundläggande rättigheterna.

Analysen avspeglar också EU-domstolens resonemang i Schremsmålet när det gäller kommissionens handlingsfrihet vid en bedömning av adekvat skyddsnivå. Kontrollen av att kraven för en adekvat skyddsnivå är uppfyllda måste utföras noggrant, med hänsyn till de grundläggande rättigheterna till privatliv och uppgiftsskydd och antalet enskilda personer som kan komma att påverkas av överföringar.

Skölden för skydd av privatlivet måste bedömas med hänsyn till dagens internationella sammanhang, t.ex. utvecklingen av stordata och det växande säkerhetsbehovet. Insamlingen och användningen av personuppgifter har ökat dramatiskt i omfattning och omfång sedan det första safe harbour-beslutet utfärdades 2000. EU:s dataskyddsmyndigheter betonar med kraft vikten av de principer som de försvarar.

Artikel 29-arbetsgruppen välkomnar för det första de stora förbättringar som skölden för skydd av privatlivet innebär jämfört med safe harbour-beslutet. Arbetsgruppen konstaterar att många av de brister i safe harbour-beslutet som den framhöll i sin skrivelse av den 10 april 2010 till kommissionens vice ordförande Viviane Reding har tagits upp av förhandlarna.

De principer och garantier som skölden för skydd av privatlivet ska medföra fastställs både i beslutet om adekvat skyddsnivå och i dess bilagor, vilket innebär att informationen är svår att hitta och ibland även är inkonsekvent. Detta bidrar till en övergripande otydlighet i det nya regelverket och innebär att det blir mer svårtillgängligt för registrerade, organisationer och

dataskyddsmyndigheter. Det språk som används är dessutom otydligt. Arbetsgruppen uppmanar därför kommissionen att göra detta tydligt och begripligt för parterna på båda sidor om Atlanten.

När det gäller den tillämpliga lagstiftningen betonar arbetsgruppen att om beslutet om huruvida skölden för skydd av privatlivet ger en adekvat skyddsnivå antas på grundval av direktiv 95/46/EG, måste det vara förenligt med EU:s rättsliga ram för uppgiftsskydd, i såväl omfattning som terminologi. Arbetsgruppen anser att det måste göras en översyn kort efter det att den allmänna dataskyddsförordningen har börjat tillämpas, för att se till att den högre skyddsnivå för personuppgifter som den förordningen innebär också tillämpas i beslutet om adekvat skyddsnivå och dess bilagor.

**Om de kommersiella aspekterna på skölden för skydd av privatlivet**

Artikel 29-arbetsgruppens viktigaste mål är att se till att enskilda personer erbjuds en skyddsnivå som är väsentligen likvärdig när personuppgifter behandlas i enlighet med bestämmelserna i skölden för skydd av privatlivet. Arbetsgruppen förväntar sig inte att skölden för skydd av privatlivet ska vara en ren och heltäckande kopia av EU:s rättsliga ram, men anser att den bör innehålla de viktigaste delarna i de grundläggande principerna och därmed säkerställa en skyddsnivå som är ”väsentligen likvärdig”.

Trots de förbättringar som skölden för skydd av privatlivet innebär, anser arbetsgruppen att vissa avgörande principer för uppgiftsskydd som fastställs i EU-lagstiftningen inte avspeglas i förslaget till beslut om adekvat skyddsnivå och dess bilagor, eller har ersatts med bristfälliga alternativa begrepp.

Principen om lagring av uppgifter anges t.ex. inte uttryckligen och framgår inte tydligt av den nuvarande ordalydelsen i principen om dataintegritet och ändamålsbegränsning. Det sägs inte heller något om det skydd som bör finnas mot automatiserade enskilda beslut som uteslutande baseras på automatiserad behandling. Det är också oklart hur principen om ändamålsbegränsning ska tillämpas på behandling av uppgifter. För att förtydliga användningen av flera viktiga begrepp föreslår arbetsgruppen att EU och Förenta staterna ska komma överens om tydliga definitioner och att dessa ska ingå i den ordlista som ska ingå i förteckningen över vanliga frågor om skölden för skydd av privatlivet.

Eftersom skölden för skydd av privatlivet också kommer att användas för att överföra uppgifter till tredjeländer kräver arbetsgruppen att vidareöverföringar från en enhet som omfattas av skölden för skydd av privatlivet till mottagare i ett tredjeland bör ge samma skyddsnivå i alla aspekter som omfattas av skölden (inklusive nationell säkerhet) och inte bör leda till lägre krav eller kringgå EU:s principer för uppgiftsskydd. Om vidareöverföring till ett tredjeland ska utföras inom ramen för skölden för skydd av privatlivet bör varje organisation som ingår i skölden vara skyldig att bedöma eventuella obligatoriska krav i tredjelandets nationella lagstiftning som är tillämpliga på uppgiftsimportören innan överföringen utförs. Rent generellt konstaterar arbetsgruppen att regelverket för vidareöverföring av EU-

personuppgifter är bristfälligt, särskilt vad avser omfattning, ändamålsbegränsning och garantier vid överföringar till förmedlare.

Arbetsgruppen konstaterar slutligen att det har införts ytterligare instanser för handläggning av klagomål, för att enskilda personer ska kunna utöva sina rättigheter. Arbetsgruppen är dock oroad över att den nya tvistlösningsmekanismen kan visa sig vara alltför komplicerad i praktiken, svår att använda för enskilda personer i EU och därför ineffektiv. Därför behövs ytterligare förtydliganden av de olika förfarandena för handläggning av klagomål. Framför allt bör EU:s dataskyddsmyndigheter, när de är villiga att göra detta, betraktas som en naturlig kontaktpunkt för enskilda personers olika förfaranden i EU och få möjlighet att agera för deras räkning.

**Undantag för ändamål som berör nationell säkerhet**

När det gäller offentliga myndigheters tillgång till uppgifter i såväl EU som i tredjeländer påminner artikel 29-arbetsgruppen om sin analys av de relevanta grundläggande rättigheterna i arbetsdokumentet om motiveringen av inskränkningar i de grundläggande rättigheterna till privatliv och uppgiftsskydd genom övervakning vid överföring av personuppgifter (grundläggande europeiska garantier) (WP237).

Ett stort framsteg jämfört med safe harbour-beslutet är att förslaget till beslut om adekvat skyddsnivå nu ingående behandlar möjligheten att få tillgång till uppgifter som behandlas inom ramen för skölden för skydd av privatlivet för ändamål som berör nationell säkerhet och brottsbekämpning. Arbetsgruppen erkänner detta viktiga steg och även den ökade insyn som Förenta staternas myndigheter erbjuder i fråga om den lagstiftning som är tillämplig på insamling av underrättelseuppgifter (bilaga VI).

Arbetsgruppen noterar dock att utfästelserna från U.S. Office of the Director of National Intelligence (ODNI) inte utesluter omfattande och urskillningslös insamling av personuppgifter med ursprung i EU. Arbetsgruppen påminner om att den sedan länge har haft uppfattningen att omfattande och urskillningslös övervakning av enskilda personer i ett demokratiskt samhälle aldrig kan anses vara proportionerlig eller absolut nödvändig, vilket krävs enligt det skydd som de tillämpliga grundläggande rättigheterna ger. Dessutom är det mycket viktigt med en omfattande tillsyn av alla övervakningsprogram. Arbetsgruppen konstaterar att det finns en tendens att samla in allt fler uppgifter i stor och urskillningslös omfattning med hänvisning till kampen mot terrorism. Med tanke på sina farhågor om vad detta innebär för skyddet av de grundläggande rättigheterna till privatliv och uppgiftsskydd ser arbetsgruppen fram emot EU-domstolens kommande avgöranden i mål som gäller omfattande och urskillningslös uppgiftsinsamling.

När det gäller prövning välkomnar arbetsgruppen inrättandet av en ombudsman som en ny prövningsmekanism. Detta kan innebära en avsevärd förbättring för EU-invånarnas rättigheter när det gäller Förenta staternas underrättelseverksamhet. Arbetsgruppen är dock oroad över att denna nya institution inte kommer att vara tillräckligt oberoende och inte få tillräckliga

befogenheter för att kunna fullgöra sitt uppdrag effektivt och att den därför inte kan garantera en tillfredsställande prövning vid tvister.

**Gemensam översyn**

Den årliga gemensamma översyn som anges i förslaget till beslut om adekvat skyddsnivå är en avgörande faktor för trovärdigheten hos skölden för skydd av privatlivet. Arbetsgruppen välkomnar varmt den möjlighet att se över beslutet om adekvat skyddsnivå som detta skulle innebära. Arbetsgruppen uppfattar det som att nationella företrädare för artikel 29-arbetsgruppen kommer att kunna delta fullt ut i granskningsprocessen, men vill ha ett förtydligande av hur arrangemanget är utformat. Villkoren (inklusive slutrapporten, hur den ska offentliggöras och eventuella konsekvenser, samt finansieringen) måste fastställas i god tid före den första granskningen.

**Slutsats**

Artikel 29-arbetsgruppen konstaterar att skölden för skydd av privatlivet innebär stora förbättringar jämfört med det ogiltigförklarade safe harbour-beslutet. Med tanke på de farhågor som arbetsgruppen gett uttryck för och de förtydliganden som den begärt, uppmanar arbetsgruppen kommissionen att ta itu med dessa farhågor, ta fram lämpliga lösningar och göra de efterfrågade förtydligandena, för att förbättra förslaget till beslut om adekvat skyddsnivå och säkerställa att den skyddsnivå som skölden för skydd av privatlivet erbjuder verkligen är väsentligen likvärdig med EU:s skyddsnivå.

**INNEHÅLLSFÖRTECKNING**

## 1. INLEDNING

Efter avgörandet i Europeiska unionens domstol (nedan kallad *EU-domstolen*) den 6 oktober 2015 i Schremsmålet[1] uppmanade artikel 29-arbetsgruppen (nedan kallad *arbetsgruppen*) Europeiska unionens medlemsstater (nedan kallade *EU*) och de andra europeiska institutionerna att inleda samtal med myndigheterna i Förenta staterna för att hitta politiska, rättsliga och tekniska lösningar för att möjliggöra överföring av uppgifter till Förenta staternas territorium och samtidigt respektera de grundläggande rättigheterna.

Efter mer än två års förhandlingar nådde Europeiska kommissionen och U.S. Department of Commerce (nedan kallat det *amerikanska handelsministeriet*) den 2 februari 2016 en politisk överenskommelse om *ett nytt regelverk för transatlantiskt utbyte av personuppgifter för kommersiella ändamål: skölden för skydd av privatlivet i EU och Förenta staterna* (nedan kallad *skölden för skydd av privatlivet*) i syfte att ersätta det tidigare safe harbour-beslutet.

Den 29 februari 2016 offentliggjorde kommissionen ett meddelande[2], ett förslag till beslut om adekvat skyddsnivå och de bilagor som ska utgöra skölden för skydd av privatlivet. I enlighet med artikel 30.1 c i direktiv 95/46/EG (nedan kallat *direktivet*) har arbetsgruppen bedömt dessa handlingar för att yttra sig om kommissionens förslag till beslut om adekvat skyddsnivå och underliggande dokument om skölden för skydd av privatlivet. Vid sin bedömning delade arbetsgruppen upp arbetet i en bedömning av den kommersiella delen av skölden för skydd av privatlivet och en bedömning av de garantier som införs i fråga om undantag från principerna för skölden för skydd av privatlivet för ändamål som berör nationell säkerhet, brottsbekämpning och allmänhetens intresse.

Efter domen i Schremsmålet har arbetsgruppen haft flera möten med delegationer från de amerikanska myndigheterna, företrädare för det civila samhällets organisationer från både EU och Förenta staterna samt akademiker, för att utarbeta sin bedömning av vilka konsekvenser domen kommer att få. Under bedömningen av skölden för skydd av privatlivet har flera möten hållits med kommissionen och företrädare för de amerikanska myndigheterna. Vid dessa möten gjordes vissa förtydliganden och dessa har beaktats i det här yttrandet. Arbetsgruppen betonar att förtydligandena vid detta skede endast har varit informella och att de inte kan betraktas som en integrerad del av förslaget till beslut om adekvat skyddsnivå, eftersom de ännu inte har lämnats skriftligt.

Arbetsgruppen välkomnar ändå särskilt att det amerikanska handelsministeriet vid dessa möten åtog sig att samarbeta med EU-medlemsstaternas dataskyddsmyndigheter i fråga om tillämpningen av skölden för skydd av privatlivet och att se till att instruktioner och rättsliga tolkningar av tillämpningen av skölden för skydd av privatlivet offentliggörs på ministeriets webbplatser.

[1] Domstolens dom av den 6 oktober 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (nedan kallad *Schremsmålet*).
[2] COM(2016)117 final av den 29 februari 2016.

## 1.1 Allmänna kommentarer

### *1.1.1 Omfattningen av arbetsgruppens bedömning*

Arbetsgruppen har först och främst beaktat det gällande regelverket för EU-medlemsstaternas uppgiftsskydd, däribland artikel 8 i Europeiska konventionen om mänskliga rättigheter (nedan kallad *Europakonventionen*) om rätten till skydd för privat- och familjeliv, samt artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) om rätten till skydd för privat- och familjeliv, rätten till skydd för personuppgifter respektive rätten till ett effektivt rättsmedel och en opartisk domstol. Arbetsguppen tog också hänsyn till gällande rättspraxis och direktivets krav.

Kravet på att ett tredjeland ska säkerställa en adekvat skyddsnivå för uppgifter definierades ytterligare av EU-domstolen i Schremsmålet. EU-domstolen förklarade inte bara att bestämmelserna i direktivet måste tolkas ”mot bakgrund av de grundläggande rättigheterna, vilka garanteras i stadgan”[3], särskilt artiklarna 7 och 8, utan påpekade också att begreppet ”adekvat skyddsnivå” ska förstås som att det ”krävs att detta tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är väsentligen likvärdig med den skyddsnivå som garanteras inom unionen enligt direktiv 95/46 jämfört med stadgan”[4]. Det gjordes aldrig en tillräckligt detaljerad bedömning av detta när det gällde det f.d. safe harbour-beslutet. Därför bedömde arbetsgruppen förslaget till beslut om adekvat skyddsnivå mot bakgrund av kravet på en analys av huruvida skyddsnivån för grundläggande fri- och rättigheter är *väsentligen likvärdig* med den skyddsnivå som garanteras inom EU. Arbetsgruppen betonar att den i detta yttrande tar upp sina viktigaste farhågor, men att nya problem kan komma att upptäckas senare, med tanke på den korta tid som har gått sedan förslaget till beslut om adekvat skyddsnivå offentliggjordes.

Arbetsgruppen erkänner att EU-domstolen genom att fastställa att ordet *adekvat* i artikel 25.6 i direktivet innebär *väsentligen likvärdig*, ytterligare har förtydligat begreppet *adekvat skyddsnivå* i Schremsmålet. Domstolen har understrukit att även om begreppet ”adekvat skyddsnivå” inte kräver att tredjelandet ska säkerställa en skyddsnivå som är identisk med den som säkerställs genom EU:s rättsordning, ska begreppet förstås som att det krävs att detta tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är *väsentligen likvärdig* med den skyddsnivå som garanteras inom unionen enligt direktiv 95/46 jämfört med stadgan.

### *1.1.2 Bedömningen av den kommersiella delen av förslaget till beslut om adekvat skyddsnivå*

Arbetsgruppen har redan förklarat hur den har tillämpat EU:s grundläggande principer för dataskydd på överföring av personuppgifter till tredjeländer i sitt arbetsdokument 12 ”Överföring av personuppgifter till tredjeland: tillämpning av artiklarna 25 och 26 i EU:s

[3] Schremsmålet, punkt 38.
[4] Schremsmålet, punkt 73.

dataskyddsdirektiv[5]. Arbetsgruppen tittade efter likvärdiga garantier som säkerställer en skyddsnivå som är likvärdig med de principer som garanteras enligt direktivet, framför allt i fråga om ändamålsbegränsning, uppgifternas kvalitet och proportionalitet, transparens, säkerhet, rätt till tillgång, rättelse och invändning, lagring av uppgifter och vidareöverföringar. En liknande metod användes i de yttranden som arbetsgruppen utfärdade vid bedömningen av beslutet om huruvida safe harbour innebar en adekvat skyddsnivå[6] och i arbetsgruppens rekommendationer i sin skrivelse till kommissionens vice ordförande och kommissionsledamot med ansvar för rättsliga frågor Viviane Reding, som offentliggjordes den 10 april 2014[7].

*1.1.3 Bedömningen av undantag för offentliga myndigheters tillgång samt deras garantier*

Bedömningen av undantag för offentliga myndigheters tillgång till personuppgifter som omfattas av skölden för skydd av privatlivet är komplex, framför allt med hänsyn till dataskyddsmyndigheternas och allmänhetens ökade medvetenhet om Förenta staternas övervakningsprogram efter Edward Snowdens avslöjanden. Arbetsgruppen erkänner och välkomnar de amerikanska myndigheternas ansträngningar för att öka insynen i övervakningsprogrammen och deras vilja att införa ytterligare garantier i skölden för skydd av privatlivet. Samtidigt betonar arbetsgruppen att alla inskränkningar i de grundläggande rättigheterna till privatliv och uppgiftsskydd måste gå att motivera i ett demokratiskt samhälle. EU-domstolen kritiserade att safe harbour-beslutet inte innehöll några slutsatser om huruvida det i Förenta staterna fanns några statligt införda regler för att begränsa eventuella inskränkningar. Inte heller hänvisas det till något effektivt rättsligt skydd mot denna typ av ingrepp.[8]

Arbetsgruppen har därför analyserat den gällande rättsliga ramen i Förenta staterna och de amerikanska underrättelseorganens praxis såsom de beskrivs i bilagorna till förslaget till beslut, samt under vilka omständigheter de medger inskränkningar i de grundläggande rättigheterna till respekt för privatliv och uppgiftsskydd, så som de skyddas enligt EU:s rättsliga ram.

För att avgöra om eventuella inskränkningar skulle gå att motivera i ett demokratiskt samhälle gjordes bedömningen mot bakgrund av EU:s rättspraxis för grundläggande rättigheter, där det fastställs fyra grundläggande garantier[9] för underrättelseverksamhet:

A. Behandling bör vara förenlig med lagen och baseras på tydliga, exakta och tillgängliga regler: detta innebär att en rimligt informerad person bör kunna förutse vad som kan hända med hans eller hennes uppgifter om de överförs.

[5] Antaget av artikel 29-arbetsgruppen den 24 juli 1998, se framför allt s. 6.
[6] Se WP62, WP32, WP27, WP23, WP21, WP19, WP15 och 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] Schremsmålet, punkterna 87 och 88.
[9] EU:s grundläggande garantier baseras på rättspraxis från EU-domstolen och Europeiska domstolen för de mänskliga rättigheterna och beskrivs närmare i arbetsgruppens arbetsdokument WP237 som offentliggjordes den 13 april 2016.

B. Nödvändighet och proportionalitet med hänsyn till de legitima mål som eftersträvas måste påvisas: det måste upprätthållas en balans mellan det syfte för vilket uppgifterna samlas in och medges tillgång för, och den enskilda personens rättigheter.
C. Det bör finnas en oberoende tillsynsmekanism som är både effektiv och opartisk: det kan vara en domare eller något annat oberoende organ, så länge de har tillräcklig förmåga att utföra de nödvändiga kontrollerna.
D. Den enskilda personen måste ha tillgång till effektiva rättsmedel: alla ska ha rätt att försvara sina rättigheter inför ett oberoende organ.

### 1.2 Förslaget till beslut om adekvat skyddsnivå

Arbetsgruppen välkomnar att ett nytt förfarande om adekvat skyddsnivå kan inledas mindre än ett halvår efter det att EU-domstolen ogiltigförklarade safe harbour-beslutet. Med tanke på den mängd uppgifter som överförs dagligen mellan EU och Förenta staterna, vilket arbetsgruppen inser är en nödvändig del av ekonomin på ömse sidor om Atlanten, bör det skapas rättslig tydlighet, ju förr desto bättre.

Arbetsgruppen beklagar dock att det förslag till beslut om adekvat skyddsnivå som kommissionen har offentliggjort inte innehåller någon heltäckande bedömning av Förenta staternas inhemska lagstiftning och internationella åtaganden i form av en rapport om huruvida skyddsnivån är adekvat, vilket tidigare har varit praxis i liknande förfaranden och är förenligt med artikel 25 i direktivet. Detta har hindrat arbetsgruppen från att göra en fullständig analys av det rättsliga sammanhanget för skölden för skydd av privatlivet. Arbetsgruppen konstaterar t.ex. att det nuvarande förslaget till beslut om adekvat skyddsnivå inte innehåller några slutsatser om den befintliga lagstiftningen för skydd av privatliv och personuppgifter i Förenta staterna på federal nivå och delstatsnivå, inklusive sektorsbaserad lagstiftning och inte heller om lagstiftning som tillåter icke-övervakningsrelaterade former av offentlig tillgång. Inte heller ges någon definition av förhållandet mellan uppgiftsöverföringar inom ramen för skölden för skydd av privatlivet och andra befintliga slutsatser om adekvat skyddsnivå, såsom avtalet mellan EU och Förenta staterna om passageraruppgifter (PNR-uppgifter) eller programmet för att spåra finansiering av terrorism (TFTP).

#### *1.2.1 Tillämpningsområde för EU:s dataskyddsregler och framför allt för principerna i direktiv 95/46/EG*

Arbetsgruppen påminner om att enligt EU:s rättsliga ram för uppgiftsskydd och framför allt enligt direktivet (artikel 4.1), ska medlemsstaternas lagar inte bara tillämpas på behandling som utförs av registeransvariga som är etablerade på deras territorium utan även när registeransvariga (trots att de inte är etablerade i EU) använder utrustning som är placerad i EU:s territorium, i synnerhet för insamling av personuppgifter. Därför är EU-medlemsstaternas lagstiftning tillämpning på all behandling som utförs före överföringen till Förenta staterna, antingen inom ramen för verksamhet inom en organisation som är etablerad i EU eller via användning av utrustning som är placerad i EU och som används av en organisation som inte är etablerad i EU. Arbetsgruppen begär att detta ska anges uttryckligen i förslaget till beslut om adekvat skyddsnivå.

Det bör framgå tydligt att principerna för skölden för skydd av privatlivet ska tillämpas från och med den tidpunkt då överföringen äger rum. Dessutom påminner arbetsgruppen om att registeransvariga som är etablerade i EU och som överför uppgifter till en registerförare i Förenta staterna fortfarande omfattas av EU:s dataskyddslagstiftning.

*1.2.2 Bristande tydlighet i handlingarna som berör skölden för skydd av privatlivet*

De principer och garantier som skölden för skydd av privatlivet ska medföra fastställs både i beslutet om adekvat skyddsnivå och i dess bilagor, vilket innebär att informationen är svår att hitta och ibland även är inkonsekvent. Detta bidrar till en övergripande otydlighet i det nya regelverket och innebär att det blir mer svårtillgängligt för registrerade, organisationer och dataskyddsmyndigheter. Det språk som används är dessutom otydligt. Arbetsgruppen uppmanar därför kommissionen att göra detta tydligt och begripligt för parterna på båda sidor om Atlanten.

Arbetsgruppen föreslår att det ska införas en särskild bilaga med definitioner av grundläggande begrepp som används i dokumenten för skölden för skydd av privatlivet. Det är avgörande med en gemensam och otvetydig förståelse av vilka skyldigheter som införs genom beslutet om huruvida skölden för skydd av privatlivet innebär en adekvat skyddsnivå för att skölden ska fungera effektivt på båda sidor om Atlanten. Därför är arbetsgruppen oroad över att de många korshänvisningarna och motstridiga formuleringarna samt de komplexa ramdokumenten kommer att leda till svårigheter i fråga om konsekvens, begriplighet och tydlighet i tillämpningen av skölden för skydd av privatlivet.

Framför allt används terminologi i dokumenten om skölden för skydd av privatlivet som inte stämmer överens med den vokabulär som används generellt i EU i samband med uppgiftsskydd. Detta behöver inte vara något problem, så länge det är tydligt vad motsvarande terminologi enligt EU-lagstiftningen (och enligt amerikansk lagstiftning) skulle vara. Arbetsgruppen beklagar dock att detta inte är fallet, inte heller i förslaget till beslut om adekvat skyddsnivå. I kapitel 3 i förslaget till beslut om adekvat skyddsnivå används t.ex. ordet *tillgång* i bemärkelsen insamling av personuppgifter, i stället för i betydelsen att någon ges möjlighet att se uppgifter som redan har samlats in. Företags tillgång till uppgifterna och de enskilda personernas rätt till tillgång är två separata begrepp som inte bör sammanblandas.

Arbetsgruppen betonar att terminologin också bör vara konsekvent i alla dokument, även i förslaget till beslut om adekvat skyddsnivå. Så är det för närvarande inte, t.ex. när det gäller begreppen *behandling* och *personuppgifter*. Båda begreppen är i princip väl definierade i bilaga II, men används inte konsekvent i alla dokument, vilket leder till kryphål i skyddet.[10,11]

[10] I vissa klausuler räknas enbart vissa typer av behandlingsaktiviteter upp, i stället för att begreppet *behandling* används. Detta skapar kryphål i skyddet. Enligt ordalydelsen i bilaga II, III.6 f skulle principerna för skölden för skydd av privatlivet t.ex. enbart vara tillämpliga när organisationen ”lagrar, behandlar eller lämnar ut” de mottagna uppgifterna (dvs. inte för andra åtgärder som omfattas av begreppet *behandling*, t.ex. insamling, registrering, ändring, hämtning, sökning, radering). Datasäkerhet skulle enbart krävas när man ”skapar, lagrar, använder eller sprider” personuppgifter (bilaga II, II.4). Definitionen av personuppgifter begränsas också till uppgifter som har ”tagits emot” och ”registrerats”. Ett annat exempel är att enligt principen om meddelande (bilaga II, II.1 a iv) måste den certifierade organisationen informera enskilda personer om de ändamål för vilka den ”samlar in och använder” uppgifter om dem. I bilaga II, III.9 a.11 nämns enbart uppgifter som

Arbetsgruppen välkomnar att definitionerna av några av de begrepp som används har tagits med i de dokument som utgör skölden för skydd av privatlivet. Detta är dock inte fallet för ett antal andra viktiga begrepp, däribland *förmedlare*, *registerförare*, *kodade uppgifter*, *avidentifierade uppgifter* och *enskild person i EU*, som arbetsgruppen anser bör ha en tydlig definition som både Förenta staterna och EU är överens om, för att undvika förvirring i ett senare skede för de registeransvariga och registerförare som använder skölden för skydd av privatlivet, tillsynsmyndigheterna och allmänheten. En enkel lösning skulle vara att lägga till en ordlista över begrepp i förteckningen över vanliga frågor om skölden för skydd av privatlivet.

Arbetsgruppen vill också nämna de legitima grunderna för behandling av känsliga uppgifter i kompletterande princip 1 (bilaga II, III.1) i fall där en organisation inte är skyldig att inhämta uttryckligt samtycke (opt in). Denna kompletterande princip 1 kan uppfattas som en förteckning över legitima grunder för uppgiftsinsamling i EU eftersom den liknar artikel 8 i direktivet. Arbetsgruppen vill påminna om att all behandling (inbegripet insamling och överföring) av känsliga uppgifter som omfattas av EU-lagstiftningen måste ske på legitima grunder enligt artikel 8 i direktivet. Skölden för skydd av privatlivet får inte tolkas som en möjlighet till alternativa grunder för en sådan behandling. Arbetsgruppen anser t.ex. att det inte är möjligt för en amerikansk organisation att samla in uppgifter som omfattas av EU-lagstiftningen på grundval av amerikansk anställningslagstiftning (se bilaga II, III.1 a v). Därför betonar arbetsgruppen att kompletterande princip 1 endast får tolkas så att den tillämpas på känsliga uppgifter som redan har överförts efter att ha samlats in i EU på legitima grunder som anges i artikel 8 i direktivet.

Slutligen konstaterar arbetsgruppen att det är oklart vem som kan betraktas som enskild person i EU och därmed omfattas av skydd inom ramen för skölden för skydd av privatlivet: alla EU-medborgare eller alla som är bosatta i EU. Detta är särskilt viktigt i samband med rätten till prövning, inbegripet tillgången till ombudsmannen. Dessutom bör beslutet om adekvat skyddsnivå ta upp frågan om i vilken omfattning skölden för skydd av privatlivet också ska tillämpas på medborgare/invånare i EES-länderna och Schweiz, som tidigare faktiskt omfattades av safe harbour-systemet.

### *1.2.3 Gemensam översyn och upphävande*

Arbetsgruppen välkomnar att kommissionen och de amerikanska myndigheterna har kommit överens om att regelbundet se över den praktiska tillämpningen av skölden för skydd av privatlivet. Denna gemensamma översyn har varit välkänd praxis i EU:s

---

”överförs” eller ”görs tillgängliga”. Även om avsikten i de flesta av dessa fall inte verkar vara att begränsa tillämpningsområdet för principerna eller skapa luckor i skyddet innebär denna inkonsekventa terminologi att det finns risk för att sådana luckor uppstår. Eftersom begreppet *behandling* definieras i principerna är det mycket viktigt att det används konsekvent för att undvika de kryphål som nu finns. Annars lämnas alltför stort utrymme för förmodat oavsiktliga tolkningar, vilket kan leda till feltolkningar av beslutets ordalydelse.

[11] I definitionen av ”personuppgifter” i bilaga II, I.8 a hänvisas till ”uppgifter om en identifierad eller identifierbar fysisk person”. I de kompletterande principerna anges dock att när det gäller personaluppgifter ska principerna endast tillämpas om ”identifierade eller identifierbara register överförs eller görs tillgängliga”. Arbetsgruppen anser att detta gör det möjligt att behandla personaluppgifter på ett sätt som inte är förenligt med principerna för uppgiftsskydd enligt EU-lagstiftningen och inte heller med den allmänna definitionen av personuppgifter i skölden för skydd av privatlivet.

dataskyddsgemenskap under ett antal år, särskilt i fråga om avtalen om överföring av PNR-uppgifter med tredjeländer och TFTP-avtalet. Arbetsgruppen välkomnar också att ett icke närmare angivet antal företrädare från dataskyddsmyndigheter kan delta i dessa gemensamma översyner.

Med tanke på sin erfarenhet av gemensamma översyner på senare år vill arbetsgruppen klargöra att den förväntar sig att den gemensamma översynen av skölden för skydd av privatlivet blir mer omfattande än de gemensamma PNR- och TFTP-översynerna. Framför allt är det önskvärt att den gemensamma översynen inte bara omfattar möten med företrädare för amerikanska myndigheter, organisationer och företag, utan att det också görs kontroller på plats av vissa delar av skölden för skydd av privatlivet. Dataskyddsmyndigheternas företrädare i den gemensamma översynen bör kunna lämna förslag till sådana kontroller på plats.

Arbetsgruppen anser att en gemensam översyn kräver en gemensam bedömning av slutsatserna. Hittills har resultatet av gemensamma översyner presenterats i arbetsdokument från kommissionens avdelningar, som inte har behövt vara godkända av de medlemmar i den gemensamma översynen som inte kommit från kommissionen. För den gemensamma översynen av skölden för skydd av privatlivet skulle arbetsgruppen uppskatta om rapporten med slutsatser verkligen blev en gemensam produkt. Som ett alternativ kan man överväga att offentliggöra en fristående gemensam översynsrapport från dataskyddsmyndigheterna.

Slutligen påminner arbetsgruppen om kommissionens löfte om att kommissionen ska ersätta kostnaderna för arbetsgruppens företrädares deltagande i gemensamma översyner. Arbetsgruppen förutsätter att detta också kommer att gälla den gemensamma översynen av skölden för skydd av privatlivet, åtminstone för ett rimligt antal företrädare från dataskyddsmyndigheterna.

Arbetsgruppen rekommenderar att villkoren för den gemensamma översynen beslutas av kommissionen, de amerikanska myndigheterna och arbetsgruppen minst tre månader innan den första gemensamma översynen av skölden för skydd av privatlivet och att de dokumenteras skriftligen.

*1.2.4 EU:s rättsliga ram under granskning*

Beslutet om huruvida ett adekvat skydd säkerställs av skölden för skydd av privatlivet är det första beslut om adekvat skyddsnivå som har utarbetats enligt den principiella överenskommelsen om texten till den allmänna dataskyddsförordningen. Arbetsgruppen har emellertid fastställt att skölden för skydd av privatlivet ännu inte avspeglar den framtida situationen. Viktiga nya begrepp, som t.ex. rätten till uppgiftsportabilitet och ytterligare skyldigheter för registeransvariga, däribland behovet att utföra konsekvensbedömningar av uppgiftsskydd och att följa principerna om inbyggt integritetsskydd och integritetsskydd som standard, har exempelvis inte införts i skölden för skydd av privatlivet. Därför föreslår arbetsgruppen att skölden för skydd av privatlivet, precis som andra befintliga beslut om adekvat skyddsnivå, ska ses över kort efter det att den allmänna dataskyddsförordningen har

trätt i kraft. Det vore lämpligt att hänvisa uttryckligen till denna översynsprocess i det slutliga beslutet om adekvat skyddsnivå.

## 2. BEDÖMNING AV DEN KOMMERSIELLA DELEN AV FÖRSLAGET TILL BESLUT OM ADEKVAT SKYDDSNIVÅ

### 2.1 Allmänna kommentarer

*2.1.1 Förbättringar*

Arbetsgruppen välkomnar de förbättringar som skölden för skydd av privatlivet innebär och förhandlarnas vilja att ta itu med de brister i safe harbour-systemet som arbetsgruppen har lyft fram. Jämfört med safe harbour har det gjorts förbättringar i följande delar: vissa viktiga definitioner har införts, t.ex. av *personuppgifter*, *behandling* och *registerförare*. Det har inrättats mekanismer för att säkerställa tillsynen av förteckningen över organisationer som är anslutna till skölden för skydd av privatlivet och det har nu blivit obligatoriskt att göra externa eller interna granskningar av efterlevnaden. Det har också gjorts förbättringar i principen om tillgång och arbetsgruppen konstaterar att det nu finns rätt att få uppgifter rättade eller borttagna när de har använts på ett sätt som inte är förenligt med principerna för skölden för skydd av privatlivet. Dessutom har det klargjorts att den enskilda personen ska få en bekräftelse av att uppgifter om honom eller henne behandlas och också underrättas om vilka uppgifter som behandlas.

Arbetsgruppen välkomnar också förstärkningen av de rättsliga garantierna vid vidareöverföringar och det amerikanska handelsministeriets och Federal Trade Commissions (FTC) åtaganden om att verkställa de skyldigheter som införs genom skölden för skydd av privatlivet.

*2.1.2 Tillämpning av skölden för skydd av privatlivet på organisationer som fungerar som registerförare (förmedlare)*

Tyvärr är det fortfarande oklart i vilken omfattning principerna för skölden för skydd av privatlivet är tillämpliga på certifierade organisationer som tar emot personuppgifter från EU enbart för registerföringsändamål (kallade *förmedlare* eller *registerförare*). I bestämmelserna i bilaga II, III.10 a nämns visserligen uppgiftsöverföringar till certifierade organisationer för sådana ändamål – dvs. kravet på att det upprättas ett avtal anges – men det anges ingenting om hur principerna för skölden för skydd av privatlivet ska tillämpas på registerförare (förmedlare). Detta skapar osäkerhet för både de certifierade amerikanska organisationer som tar emot uppgifter för registerföringsändamål, de EU-företag som gör dataöverföringar till certifierade organisationer som fungerar som registerförare och de enskilda personer vars uppgifter behandlas. Därför blir det svårt att avgöra vilka skyldigheter som verkligen gäller för organisationer som omfattas av skölden för skydd av privatlivet när de behandlar personuppgifter som de tar emot av EU i sin roll som registerförare. Här krävs det alltså verkligen ett förtydligande.

Flera av de skyldigheter som ingår i principerna är inte lämpliga för registerförare, eftersom det alltid är den registeransvarige som fastställer ändamålen och metoderna för uppgiftsbehandlingen (jfr. definitionen av *registeransvarig* i bilaga II, I.8 c). Därför kan vissa skyldigheter som fastställs i principerna, om de tillämpas på en organisation som agerar som förmedlare, stå i strid med det behandlingsavtal som krävs enligt EU-lagstiftningen (det avtal som avses i bilaga II, III.10 a). Behandlingsavtalet kommer t.ex. i allmänhet inte att ge registerföraren (förmedlaren) tillstånd att vidareöverföra uppgifter till registerförare som är en tredje part, ens under de omständigheter som anges i bilaga II, II.3 a. Vidareöverföring av uppgifter till förmedlare som är en tredje part bör endast vara tillåtet efter förhandstillstånd från den registeransvarige. Enligt EU-lagstiftningens krav kommer en registerförare (förmedlare) dessutom inte att kunna ge enskilda personer fullständiga meddelanden så som är avsikten med principen om meddelande (bilaga II, II.1), bland annat för att denna organisation inte avgör vilka ändamål behandlingen utförs för.

Därför är det mycket viktigt att förtydliga i principerna att bestämmelserna i behandlingsavtalet och framför allt instruktionerna från den organisation som överför uppgifterna ut från EU ska ha företräde när den här typen av motsägelser uppstår. Utan ett sådant förtydligande kan principerna tolkas och tillämpas på ett sätt som ger registerföraren som omfattas av skölden för skydd av privatlivet alltför stora kontrollmöjligheter och detta skulle innebära att uppgiftsexportören i EU riskerar att bryta mot sina skyldigheter som registeransvarig enligt EU:s dataskyddslagstiftning, som exportören omfattas av när den överför uppgifter till en organisation som omfattas av skölden för skydd av privatlivet och som agerar som förmedlare. Dessutom ger denna otydlighet intryck av att registerföraren får återanvända uppgifterna enligt egna önskemål.

Vidare bör det fastställas särskilda regler för det fall när en organisation agerar som registerförare (förmedlare), för att se till att organisationen följer den registeransvariges instruktioner. Det bör klargöras att amerikanska organisationer som tar emot uppgifter för rena registerföringsändamål inte får besluta att behandla uppgifterna för egen räkning. Utan särskilda regler som är tillämpliga på organisationer som agerar som registerförare är det svårt att avgöra vilka regler som registerföraren (förmedlaren) ska kunna utföra sin självcertifiering gentemot.

### *2.1.3 Begränsningar av skyldigheten att följa principerna*

I bilaga II, I.5 föreskrivs bl.a. undantag från principerna när uppgifter som omfattas av skölden för skydd av privatlivet används för ändamål som berör nationell säkerhet[12], allmänna intressen, brottsbekämpning eller krävs enligt lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter. Utan fullständig kännedom om amerikansk lagstiftning på såväl federal som delstatlig nivå är det svårt för arbetsgruppen att bedöma omfattningen av detta undantag och avgöra om dessa begränsningar är motiverade i ett demokratiskt samhälle. Det är mycket viktigt att kommissionen i sitt förslag till beslut om adekvat skyddsnivå också tar med en analys av skyddsnivån när dessa

[12] Se kapitel 3 för fler kommentarer om användningen av personuppgifter som omfattas av skölden för skydd av privatlivet för ändamål som berör nationell säkerhet och kapitel 4 för ändamål som berör brottsbekämpning.

undantag tillämpas. Arbetsgruppen uppmanar kommissionen att se till att EU informeras om eventuella lagar eller myndighetsföreskrifter som kan påverka efterlevnaden av principerna och som är tillämpliga just nu, eller som kommer att vara tillämpliga när de nya lagarna eller föreskrifterna träder i kraft i Förenta staterna.

*2.1.4 Avsaknad av princip om begränsning av lagring av uppgifter*

Principen om begränsning av lagring av uppgifter (artikel 6.1 e i direktivet) är grundläggande i EU:s dataskyddslagstiftning. Den innebär att personuppgifter endast ska förvaras så länge det är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades.

I de dokument som utgör skölden för skydd av privatlivet kan arbetsgruppen dock inte hitta någon hänvisning till att registeransvariga måste se till att uppgifterna raderas när det ändamål för vilket de insamlades eller vidarebehandlades har upphört att gälla. Därför verkar principerna inte införa någon begränsning för hur länge de certifierade organisationerna får lagra uppgifterna som liknar det som krävs enligt principen om begränsning av uppgiftslagring enligt EU-lagstiftningen.

Formuleringen av principen om dataintegritet och ändamålsbegränsning (bilaga II, II.5) kan inte på något sätt anses medföra en skyldighet för en organisation som fungerar som registeransvarig att radera uppgifter när de inte längre är nödvändiga för det ändamål för vilket de har samlats in eller för vilket de senare har behandlats, eller för en organisation som fungerar som registerförare att radera uppgifter efter det att tjänsteavtalet har upphört att gälla.

Arbetsgruppen betonar att avsaknaden av bestämmelser om en gräns för lagringen av uppgifter inom ramen för skölden för skydd av privatlivet ger organisationer möjlighet att lagra uppgifter så länge de vill, även efter det att de har lämnat skölden för skydd av privatlivet, vilket inte är förenligt med den grundläggande principen om begränsning av lagring av uppgifter.

*2.1.5 Inga garantier i fråga om automatiserade beslut som ger rättsliga effekter eller påverkar den enskilda personen märkbart*

Skölden för skydd av privatlivet ger inga rättsliga garantier när enskilda personer blir föremål för ett beslut som har rättsliga följder för dem eller som märkbart påverkar dem och som enbart grundas på automatisk behandling av uppgifter som är avsedda att bedöma vissa personliga egenskaper hos den berörda personen, exempelvis arbetsprestationer, kreditvärdighet, pålitlighet och uppträdande.

Arbetsgruppen framhöll behovet av att införa rättsliga garantier i fråga om automatiserade beslut (som ger rättsliga effekter eller påverkar den enskilda personen märkbart) för att ge en adekvat skyddsnivå redan i sitt arbetsdokument 12.

Detta behov blir desto viktigare eftersom den konstanta teknikutvecklingen gör att fler företag kan överväga att införa automatiska beslutssystem som kan försvaga enskilda personers

ställning och innebära att de saknar möjlighet att göra invändningar mot dessa datorgenererade beslut. När beslut som fattats helt och hållet av sådana automatiserade system påverkar enskilda personers rättsliga situation eller påverkar dem märkbart på annat sätt (genom t.ex. svartlistning där enskilda personer berövas sina rättigheter) är det oerhört viktigt att det finns tillräckliga skyddsmekanismer, däribland rätten att få information om den underliggande logiken och att begära omprövning på icke-automatiserade grunder.

*2.1.6 Övergångsperiod för befintliga kommersiella förbindelser*

Enligt skölden för skydd av privatlivet ska principerna tillämpas omedelbart, från och med certifieringen. Organisationer som certifierar sig inom de två första månaderna efter det att skölden för skydd av privatlivet har trätt i kraft kommer emellertid att behöva anpassa eventuella befintliga kommersiella förbindelser med tredje part efter principen om ansvar för vidare överföring så snart som möjligt. De bör under alla omständigheter göra detta inom nio månader från den dag då de certifierar sig enligt skölden för skydd av privatlivet.

Detta innebär att befintliga avtal kommer att behöva anpassas efter principerna någon gång mellan två och nio månader efter certifieringen. Under denna övergångsperiod räcker det med att uppfylla principerna om meddelande och valmöjlighet. Arbetsgruppen betonar kraftigt att överföringar inte får utföras på grundval av skölden för skydd av privatlivet förrän organisationen fullt ut kan uppfylla samtliga krav som skölden innebär. En möjlighet att skicka uppgifter under en övergångsperiod utan att mottagaren kan följa principerna för skölden för skydd av privatlivet fullt ut kan inte anses uppfylla villkoren för en laglig överföring och är därför inte acceptabel.

**2.2 Särskilda kommentarer**

*2.2.1 Insyn*

a) Allmänna anmärkningar om principen om meddelande

Arbetsgruppen välkomnar de mer omfattande och detaljerade krav som anges i principen om meddelande, särskilt att meddelandet måste innehålla en länk eller webbadress till förteckningen över organisationer som har anslutit sig till skölden för skydd av privatlivet samt en hänvisning till enskilda personers rätt till tillgång och alternativa tvistlösningsmekanismer.[13] Arbetsgruppen föreslår dock en tydligare beskrivning av de övriga rättigheter (rätten att korrigera eller radera uppgifter som är felaktiga eller som behandlats i strid mot principerna).

De dokument som bildar skölden för skydd av privatlivet väcker frågor om vid vilken tidpunkt en organisation som är ansluten till skölden för skydd av privatlivet måste meddela en enskild person. I bilaga II, II.1 b anges att detta ”meddelande (...) ska lämnas vid det tillfälle då den enskilde för första gången ombes lämna personuppgifter till en viss

[13] Bilaga II, II.1. Arbetsgruppen hänvisar också till kommissionens andra rekommendation i meddelande COM(2103)847 och arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2041, framför allt punkt 4 under ”Insyn”.

organisation eller så snart därefter det är praktiskt möjligt, men i alla händelser innan organisationen använder sådana uppgifter för ett annat ändamål än det för vilket de ursprungligen insamlades eller behandlades av den organisation som överför uppgifterna eller lämnar ut dem till tredje part för första gången". Arbetsgruppen anser att en amerikansk organisation som är ansluten till skölden för skydd av privatlivet i många fall inte kommer att samla in uppgifter direkt från den registrerade, varför meddelandet bör lämnas vid det tillfälle då uppgifterna registreras av den organisation som är ansluten till skölden för skydd av privatlivet.

Arbetsgruppen konstaterar att den faktiska tillämpningen av kraven i fråga om principen om meddelande och integritetsskyddspolicy bör bedömas vid den första årliga översynen av skölden för skydd av privatlivet.

b) Offentlig tillgång till integritetsskyddspolicy

Arbetsgruppen välkomnar att det nu uttryckligen anges att handelsministeriet ska kontrollera att företagen har offentliggjort sin integritetsskyddspolicy på sin webbplats, eller, om de saknar offentlig webbplats, var integritetsskyddspolicyn har gjorts tillgänglig för allmänheten.[14]

c) Offentliggörande av integritetsskyddsvillkor i avtal med registerförare

Bland de villkor som anges i skölden för skydd av privatlivet för att organisationer som är anslutna till skölden ska få överföra uppgifter till en registerförare (förmedlare) ingår att självcertifierade organisationer på begäran ska lämna "en sammanfattning eller en representativ kopia av de relevanta integritetsskyddsbestämmelserna i sitt avtal med förmedlaren till myndigheten" (se bilaga II, II. 3 b v). Arbetsgruppen välkomnar detta insynskrav på handelsministeriet.

*2.2.2 Valmöjlighet*

I skölden för skydd av privatlivet ingår en rätt att välja (opt out) om personuppgifter ska lämnas till en tredje part eller användas för ett väsentligt annorlunda ändamål[15] (bilaga II, III, 2). Dessutom har enskilda personer rätt att när som helst kunna välja att undanbe sig att personuppgifter används för direktmarknadsföring (bilaga II, III.12 a)[16].

Med undantag för ändamål som berör direktmarknadsföring anges inga närmare detaljer om hur och när denna valmöjlighet kan utövas. Arbetsgruppen anser att det inte räcker med att göra en enkel hänvisning till att denna rätt finns i integritetsskyddspolicyn. I stället borde den *enskilda personen* erbjudas möjlighet att utöva denna rätt *innan* personuppgifter lämnas eller återanvänds.

[14] Se de första rekommendationerna från kommissionen i dess meddelande COM(2013)847 och arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014, framför allt punkt 3 under "Insyn".
[15] Enligt kompletterande princip 14 c I får deltagare när som helst besluta sig för eller uppmanas att dra sig ur ett kliniskt försök, vilket kan betraktas som rätten att göra invändningar eller att dra tillbaka sitt samtycke.
[16] Detta är identiskt med vad som föreskrevs i safe harbour-systemet (vanlig fråga nr 12) och det har inte gjorts några ändringar i detta avseende.

Dessutom betonar arbetsgruppen att en allmän rätt att göra invändningar (på avgörande skäl som avser den registrerades särskilda situation), dvs. att den registrerade ska ha rätt att begära att behandlingen av dennes uppgifter ska avbrytas när det finns avgörande skäl som avser den registrerades särskilda situation, bör erbjudas inom ramen för skölden för skydd av privatlivet[17]. Arbetsgruppen rekommenderar starkt att det i förslaget till beslut om adekvat skyddsnivå klargörs att rätten att göra invändningar bör föreligga vid varje enskild tidpunkt och att denna invändning inte ska begränsas till uppgifternas användning för direktmarknadsföring[18].

Arbetsgruppen är oroad över att avsaknaden av en definition av vad som ska anses vara ändamål som ”väsentligen skiljer” sig från det ursprungliga ändamålet kommer att leda till förvirring och rättslig osäkerhet. Det bör förtydligas att principen om valmöjlighet under alla omständigheter inte får användas för att kringgå principen om ändamålsbegränsning[19]. Valmöjligheten bör endast vara tillämplig om ändamålet i sak skiljer sig från, men fortfarande är förenligt med det ursprungliga ändamålet, eftersom det är förbjudet med behandling för oförenliga ändamål (bilaga II, II.5 a). Det måste förtydligas att rätten att välja (opt out) inte får ge organisationen möjlighet att använda uppgifter för oförenliga ändamål. Därför rekommenderar arbetsgruppen att formuleringarna harmoniseras och att en gemensam och definierad ordalydelse används (t.ex. ”ändamål som skiljer sig i sak men som är förenliga”).

Det skulle underlätta med ett förtydligande av huruvida ett beslut om att behandla uppgifter för ett annat ändamål eller om att lämna ut uppgifter omfattas av EU-lagstiftningen. I den situationen skulle de vanliga villkoren enligt EU-lagstiftningen för sådan behandling (t.ex. förbudet mot behandling för oförenliga ändamål, kravet på att det ska finnas legitim grund för behandlingen och behovet av att meddela den enskilda personen) vara direkt tillämpliga även på den amerikanska organisation som omfattas av EU-lagstiftningens tillämpningsområde. I praktiken innebär detta att det är den EU-exportör som fattar ett sådant beslut som ska säkerställa insyn och laglighet i behandlingen enligt EU-lagstiftningen. Principen om valmöjlighet kommer endast att vara tillämplig när beslutet uteslutande fattas av den amerikanska organisation som är ansluten till skölden för skydd av privatlivet och som inte omfattas av EU-lagstiftningen.

*2.2.3 Vidare överföringar*

a) Tillämpningsområde

Arbetsgruppen är oroad över situationen där vidare överföringar av personuppgifter görs från en amerikansk certifierad organisation som är ansluten till skölden för skydd av privatlivet till en mottagare i tredjeland.

Skölden för skydd av privatlivet bör inte bara betraktas som ett verktyg för att överföra EU-uppgifter från EU till Förenta staterna, utan kommer också att fungera som ett verktyg för att

[18] Se arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding, under ”Valmöjlighet”.
[19] Ett konkret exempel på oförenlig vidare behandling som är tillåten enligt principen om valmöjlighet återfinns i kompletterande princip 9 b i (se arbetsgruppens kommentar om den under punkten som avser personaluppgifter).

föra över uppgifter från Förenta staterna till tredjeländer. Därför är bestämmelser om vidare överföringar en viktig del i skölden för skydd av privatlivet och bör ge tillräckliga garantier och en adekvat skyddsnivå när uppgifter överförs vidare utanför Förenta staterna. En särskild fråga handlar om nationell säkerhet och brottsbekämpning.

Principen om ansvar för vidare överföring i skölden för skydd av privatlivet är inte begränsad till mottagande registeransvariga, registerförare eller förmedlare som är etablerade i Förenta staterna. Därför skulle vidare överföring till tredjeland kunna göras på grundval av skölden för skydd av privatlivet, även om tredjelandet har lagar som föreskriver offentlig tillgång till personuppgifter, t.ex. för övervakningsändamål. Detta innebär en risk för att uppgifter från EU utsätts för oberättigade inskränkningar av skyddet för de grundläggande rättigheterna.

Vid varje fall av vidare överföring till tredjeland bör varje organisation som är ansluten till skölden för skydd av privatlivet vara skyldig att bedöma de obligatoriska krav i tredjelandets nationella lagstiftning som är tillämpliga på uppgiftsimportören innan överföringen utförs. Om den amerikanska organisation som är ansluten till skölden för skydd av privatlivet och som agerar som registerförare (förmedlare) upptäcker att det finns risk för påtagligt negativa effekter på de garantier, skyldigheter och skyddsnivåer som skölden för skydd av privatlivet innebär, ska organisationen utan dröjsmål meddela den registeransvariga i EU innan någon vidare överföring görs. I dessa fall har dataexportören rätt att avbryta överföringen av uppgifter och/eller upphäva avtalet. Om det finns en sådan risk för påtagligt negativa effekter bör en organisation som är ansluten till skölden för skydd av privatlivet och som agerar som registeransvarig inte få tillstånd att vidare överföra uppgifterna, eftersom detta skulle strida mot organisationens skyldighet att erbjuda samma skyddsnivå som anges i principerna vid vidare överföringar (se bilaga II, II.3 a).

Om tredjelandets lagstiftning ändras på ett sätt som sannolikt kommer att få påtagligt negativa effekter för de garantier, skyldigheter och skyddsnivåer som skölden för skydd av privatlivet innebär bör den amerikanska organisation som är ansluten till skölden för skydd av privatlivet och som agerar som registerförare (förmedlare) vara skyldig – enligt skölden för skydd av privatlivet – att så snart den blir medveten om denna ändring underrätta dataexportören om den. I det fallet har dataexportören rätt att avbryta överföringen av uppgifter och/eller upphäva avtalet. I sådant fall bör en organisation som är ansluten till skölden för skydd av privatlivet och som agerar som registeransvarig alltså inte få tillstånd att göra vidare överföringar, eftersom den är skyldig att erbjuda samma skyddsnivå som anges i principerna vid vidare överföringar (se bilaga II, II.3 a).

Arbetsgruppen påminner om sin ståndpunkt att om den registeransvarige i EU känner till en vidare överföring till en tredje part utanför Förenta staterna redan innan överföringen till Förenta staterna sker, eller om den registeransvarige i EU har gemensamt ansvar för beslutet att tillåta vidare överföringar, ska överföringen betraktas som en direkt överföring från EU till tredjelandet utanför Förenta staterna. Detta innebär att artiklarna 25 och 26 i direktivet är tillämpliga på överföringen i stället för principen om vidare överföring enligt skölden för skydd av privatlivet.

b) Överföringar från en organisation som är ansluten till skölden för skydd av privatlivet till en registeransvarig hos tredje part.

Arbetsgruppen välkomnar skyldigheten att upprätta avtal (bilaga II, II. a) för att se till att den registeransvarige hos tredje part kommer att ge åtminstone samma skyddsnivå som krävs enligt principerna för skölden för skydd av privatlivet. Syftet är att se till att personuppgifter fortsätter att ha ett adekvat skydd även efter en vidare överföring. Arbetsgruppen har dock vissa synpunkter på de föreslagna villkoren.

Saknad hänvisning till principen om ändamålsbegränsning

Arbetsgruppen rekommenderar att det också införs en tydlig hänvisning till principen om ändamålsbegränsning (bilaga II, II.5) i villkoren för vidare överföring till en registeransvarig hos tredje part (bilaga II, II.3 a). Detta skulle klargöra att vidare överföringar inte får göras om den registeransvarige hos den tredje parten kommer att behandla uppgifterna för ett oförenligt ändamål.

Undantag från kravet på avtal vid koncerninterna överföringar mellan registeransvariga

Det införs ett undantag från kravet på avtal vid koncerninterna överföringar mellan registeransvariga. I det här fallet anges i principerna att bindande företagsregler eller ”andra koncerninterna instrument (t.ex. efterlevnads- och kontrollprogram)” ska användas för att garantera att skyddet fortsätter att gälla (bilaga II, III.10 b). Arbetsgruppen anser att hänvisningen till ”andra koncerninterna instrument” inte garanterar rättsligt bindande åtaganden från de andra medlemmarna i koncernen. Eftersom arbetsgruppen och EU-lagstiftningen[20] i allmänhet förordar bindande åtaganden i fråga om koncerninterna överföringar är det viktigt att undvika att skölden för skydd av privatlivet används som ett sätt att kringgå det kravet. Arbetsgruppen påminner om att vidare överföringar från Förenta staterna till tredjeländer som är planerade redan innan överföringen till Förenta staterna äger rum, eller som omfattas av gemensamt registeransvar med den registeransvarige i EU[21], under alla omständigheter måste betraktas som en direkt överföring från EU till tredjelandet utanför Förenta staterna. Artiklarna 25 och 26 i direktivet är därför tillämpliga på överföringen.

c) Överföringar från en organisation som är ansluten till skölden för skydd av privatlivet till en registerförare (förmedlare) hos tredje part

Arbetsgruppen välkomnar att det nu är obligatoriskt med ett avtal för vidare överföringar för mottagande enheter som agerar som registerförare (förmedlare) oavsett om de är anslutna till skölden för skydd av privatlivet eller om de omfattas av någon annan lösning som garanterar adekvat skyddsnivå. Arbetsgruppen välkomnar också de ytterligare garantierna för dessa vidare överföringar (bilaga II, II.3 a i, II.3 a iii, II.3 a iv, II.3 a v, II.7 d). Den sista punkten (bilaga II, II.7 d) gäller skyldigheten att behålla ansvaret när uppgifter lämnas till en förmedlare. Det verkar dock som om denna garanti inte kommer att gälla om en organisation

[20] Behovet av bindande åtaganden som går att verkställa understryks också i den allmänna dataskyddsförordningen, oavsett vilket verktyg som används (bindande företagsregler, avtalsklausuler, uppförandekoder eller certifiering).
[21] T.ex. för personaluppgifter.

har valt att samarbeta med en dataskyddsmyndighet (se bilaga II, III.5 a). Arbetsgruppen förstår inte skälet till ett sådant undantag och anser att ansvarsskyldigheten bör tillämpas även i detta fall.

Saknad hänvisning till principen om ändamålsbegränsning

Arbetsgruppen konstaterar att enligt principen om ansvar för vidare överföring (bilaga II, II.3) får personuppgifter endast överföras till en tredje part som agerar som förmedlare för begränsade och angivna ändamål, men att det inte uttryckligen anges att dessa begränsade och angivna ändamål måste vara förenliga med de ursprungliga ändamål för vilka uppgifterna samlades in och med den registeransvariges instruktioner. Denna punkt behöver förtydligas. Därför föreslår arbetsgruppen att förslaget till beslut om adekvat skyddsnivå ska göras mer detaljerat, t.ex. genom att det införs en tydlig hänvisning till principen om ändamålsbegränsning (bilaga II, II.5) som innebär att uppgifter inte får behandlas (inbegripet lämnas ut) för oförenliga ändamål inom ramen för principen om vidare överföringar (i tillägg till principen om valmöjlighet).

Behov av fler kompletterande skyldigheter för organisationer som är anslutna till skölden för skydd av privatlivet och som agerar som registerförare (förmedlare) och vidareöverför uppgifter till en annan registerförare (förmedlare)

Bristen på tydliga regler när den organisation som är ansluten till skölden för skydd av privatlivet agerar som förmedlare (dvs. för en EU-registeransvarigs räkning) skapar ett kryphål och kan innebära att den registeransvariga i EU inte kan behålla kontrollen. En organisation som är ansluten till skölden för skydd av privatlivet och som tar emot uppgifterna i egenskap av registerförare för en registeransvarig i EU måste följa den registeransvariges instruktioner. Detta bör anges uttryckligen i principerna för att se till att bristande efterlevnad av dessa instruktioner inte bara är ett avtalsbrott (bilaga II, III.10 a ii) utan också bryter mot principerna för skölden för skydd av privatlivet.

Möjligheten för en organisation som är ansluten till skölden för skydd av privatlivet och som fungerar som förmedlare att senare överföra uppgifter till en förmedlare hos tredje part måste framgå för den registeransvarige och måste godkännas i förväg av denne. Det bör därför tydligt anges att det är förmedlarens avtal med den registeransvarige i EU (kallas i vanlig fråga 10 för *artikel 17-avtalet*) som avgör om det är tillåtet med en vidare överföring.[22]

De nuvarande villkor som är tillämpliga på vidareöverföringen till en förmedlare bygger på antagandet att den organisation som är ansluten till skölden för skydd av privatlivet fungerar som registeransvarig och därmed själv kan besluta om ett eventuellt ingripande av en agent hos en tredje part. Detta bör dock inte vara möjligt när en organisation som är ansluten till skölden fungerar som förmedlare. Annars kommer den registeransvarige i EU att fråntas sin kontrollförmåga.

[22] Se arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014, punkt 4 under ”Vidare överföring”.

De relevanta integritetsskyddsbestämmelserna i avtalet med förmedlaren hos en tredje part måste göras tillgängliga för den registeransvarige och måste ge minst samma skyddsnivå som föreskrivs i avtalet med den registeransvarige.

*2.2.4 Dataintegritet och ändamålsbegränsning*

a) Proportionalitetsprincipen

Arbetsgruppen hänvisar till sin skrivelse till kommissionens vice ordförande Viviane Reding, där den skrev att ”behandling av personuppgifter skulle även när principen om meddelande och valmöjlighet följs strikt kunna vara oproportionerlig i förhållande till den registrerades eller samhällets intresse av fri- och rättigheter. Proportionalitetsprincipen och principen om rimlighet måste följas i alla steg i behandlingen och bör vara tillämplig i tillägg till principerna om meddelande och valmöjlighet”[23].

Enligt skölden för skydd av privatlivet (bilaga II, II.5 a) måste uppgifterna begränsas till vad som är relevant för behandlingen. Arbetsgruppen skulle föredra att denna formulering ändras i det slutliga beslutet om adekvat skyddsnivå, eftersom enbart det faktum att uppgifterna är relevanta för behandlingen inte är tillräckligt för att behandlingen ska vara proportionerlig. För att uppfylla proportionalitetsprincipen bör behandlingen begränsas till de uppgifter som är nödvändiga för den berörda behandlingen.

b) Tillförlitlighet

I principen om dataintegritet och ändamålsbegränsning (bilaga II, II.5) anges också följande: ”I den omfattning som krävs för dessa ändamål måste en organisation vidta nödvändiga åtgärder för att se till att personuppgifterna är tillförlitliga för det avsedda ändamålet samt riktiga, fullständiga och aktuella.” Arbetsgruppen konstaterar att det är exakt samma formulering som används i safe harbour-systemet. Arbetsgruppen ifrågasätter att orden ”i den omfattning som krävs för dessa ändamål” bör vara med, eftersom den anser att uppgifternas tillförlitlighet inte bör vara beroende av ändamålet med behandlingen. Arbetsgruppen skulle föredra att denna koppling inte görs i det slutliga beslutet om adekvat skyddsnivå.

c) Ändamålsbegränsning

När personuppgifter överförs till en amerikansk organisation av en registeransvarig som är etablerad i EU bör exportören av uppgifter uttryckligen informera den amerikanska organisationen om de ändamål för vilka uppgifterna ursprungligen har samlats in. Detta är nödvändigt för att avgöra om ändamålet förändras efter överföringen och på så sätt utlöser principerna om meddelande och valmöjlighet. Detta skulle bidra till fördelningen av risker och ansvar.

Enligt principen om dataintegritet och ändamålsbegränsning (bilaga II, II.5) får en organisation inte behandla personuppgifter på ett sätt som är oförenligt med de ändamål för

[23] Se arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014, s. 8.

vilka uppgifterna samlades eller som den enskilda personen i efterhand har gett sitt tillstånd till. Principen om valmöjlighet (bilaga II, II.2) innebär dock att samtycke (opt-in) ska lämnas för ”användning” av känsliga uppgifter (dvs. personuppgifter som rör medicinska förhållanden och hälsa, ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter rörande sexualliv) för ändamål som väsentligen skiljer sig från de ändamål för vilka de ursprungligen samlades in eller som den enskilda personen i efterhand har gett sitt tillstånd till. Detta krav på samtycke ställs inte i de situationer som anges i kompletterande princip 1 a (bilaga II, III.1 a). När det gäller icke känsliga personuppgifter införs en rätt att välja att inte delta (opt-out).

Arbetsgruppen konstaterar att principen om ändamålsbegränsning har en annan räckvidd enligt principerna om meddelande, valmöjlighet och dataintegritet och ändamålsbegränsning. Begreppen *oförenligt ändamål* och *ändamål som väsentligen skiljer sig* används inom samma text utan någon tydligt definition[24].

Arbetsgruppen är allvarligt oroad över att denna brist på konsekvens kan leda till stora svårigheter att förena principen om dataintegritet och ändamålsbegränsning (bilaga II, II.5) med principen om valmöjlighet (bilaga II, II.2), eftersom den ena fastställer att uppgifter inte får behandlas på ett sätt som är oförenligt med syftet för vilka de samlades in, medan den andra innebär en rätt att välja att inte delta (opt-out) om uppgifter behandlas för ett ändamål som väsentligen skiljer sig från det syfte/de syften för vilka de ursprungligen insamlades.

Det betyder att principen om valmöjlighet kan uppfattas som ett godkännande av vidare oförenlig behandling[25]. Arbetsgruppen menar att det måste anges uttryckligen att en organisation inte ska få behandla uppgifter för ett ändamål som väsentligen skiljer sig från det syfte/de syften för vilka de ursprungligen insamlades, om detta ändamål är oförenligt enligt principen om ändamålsbegränsning. Det bör med andra ord klargöras att principen om valmöjlighet inte innebär ett undantag från ändamålsbegränsningen.

Om vidare behandling kan anses vara förenlig med det ursprungliga ändamålet bör dessutom principerna om meddelande och valmöjlighet tillämpas.

### *2.2.5 Journalistiska undantag*

De journalistiska undantagen för behandling av personuppgifter tas upp i kompletterande princip 2 (bilaga II, III.2). Dessa bestämmelser avspeglar den amerikanska konstitutionens skydd för yttrandefriheten. Därför anges i dokumenten som ingår i skölden för skydd av privatlivet att personuppgifter ”som återfinns i tidigare offentliggjort stoff som sprids från mediers arkiv [inte omfattas] av kraven enligt sköldens principer” (bilaga II, III.2 b). Detta undantag verkar omfatta all eventuell vidare behandling av någon registeransvarig eller

[24] Arbetsgruppen konstaterar att även vissa andra uttryck används: ”en användning som inte är förenlig med” (bilaga II, III.14 b ii), ”användning för andra ändamål” (bilaga II, III. 9 b i), användning för ”ett annat ändamål än det för vilket de ursprungligen insamlades eller behandlades” (bilaga II, II.1 b). Denna otydlighet kan leda till att det saknas tillräckliga garantier för principen om ändamålsbegränsning.

[25] Se även kommentaren under principen om valmöjlighet. Arbetsgruppen anser att risken för en sådan tolkning ökar på grund av att reglerna för vidare överföring (bilaga II, II.3) endast hänvisar till principen om valmöjlighet och inte till principen om ändamålsbegränsning.

registerförare, dvs. det är inte begränsat till vidare behandling för journalistiska ändamål. Som redan anges i skrivelsen till kommissionens vice ordförande Viviane Reding av den 10 april 2014, skulle arbetsgruppen ha föredragit en mer begränsad strategi för journalistiska undantag, som låg mer i linje med den princip som tillämpas i EU och med rätten att strykas ur förteckningar efter domen i målet om Google Spain[26].

*2.2.5 Registrerades rätt till tillgång, korrigering och radering*

Enligt skölden för skydd av privatlivet har enskilda personer rätt att få *bekräftelse* på om en organisation behandlar deras uppgifter och organisationen ska *meddela dem* vilka uppgifter som behandlas (bilaga II, III.8 a i). Organisationernas skyldighet att besvara förfrågningar från enskilda personer om behandlingens ändamål, vilka kategorier av personuppgifter som berörs och om vilka mottagare eller kategorier av mottagare som personuppgifterna lämnas ut till är förhållandevis svag. Arbetsgruppen anser att de närmare föreskrifterna om vad som ska lämnas ut till den registrerade bör anges i huvudtexten och inte enbart i en fotnot. Dessutom bör de utformas som en tydlig skyldighet (kopplad till bilaga II, III.8 a i 1).

Enligt kompletterande princip 8 behöver tillgång ”bara medges i den mån en organisation lagrar personuppgifterna” (bilaga II, III.8 d ii). Denna regel bör inte tolkas restriktivt, dvs. tillgång måste i princip medges för uppgifter som behandlas på något sätt av en organisation, och inte enbart för sådana uppgifter som lagras. För att rätten till tillgång ska vara effektiv är det därför viktigt att förtydliga att med ”lagring” avses ”behandling” i den mening som fastställs i definitionen i bilaga II, I.8 b. Tillämpningen av denna regel bör undersökas noggrant vid den gemensamma översynen av skölden för skydd av privatlivet.

Det finns fortfarande farhågor om förteckningen över undantag i bilaga II, III.8 e i, som liknar den som anges i vanlig fråga nr 8 i safe harbour-systemet och som tenderar att ge större vikt åt organisationernas intressen. Här kan enskilda personer nekas tillgång till sina egna personuppgifter av följande skäl: ”brott mot yrkesmässiga privilegier eller skyldigheter” (bilaga II, III.8 e.3), ”försvåra säkerhetskontroller som gäller anställda eller klagomålsförfaranden eller i samband med turordning när det gäller personplanering och omstrukturering av organisationer” (bilaga II, III.8 e.4) och ”skada den konfidentialitet som kan vara nödvändig i samband med övervakning, inspektion eller reglerande funktioner som tillhör en sund ekonomisk eller finansiell förvaltning, eller i framtida eller pågående förhandlingar som berör organisationen” (bilaga II, III.8 e.5). Dessa skäl bör läsas i tillägg till det allmänna undantag för konfidentiella uppgifter om affärsverksamhet som anges i bilaga II, III.8 c. Det innebär att en enskild person aldrig kommer att få tillgång till sina uppgifter i de situationer som anges ovan. Det skapas ingen balans mellan den enskilda personens och organisationens rättigheter och skyldigheter i samband med förfrågan om tillgång.

Arbetsgruppen påminner om att enskilda personer har rätt att få tillgång till sina egna uppgifter i enlighet med artikel 8.2 i stadgan. Denna rättighet är visserligen inte absolut, men

[26] Domstolens dom av den 13 maj 2014, Google Spain/Agencia Española de Protección de Datos and Mario Costeja González, C-131/12, ECLI:EU:C:2014:317.

den är grundläggande för rätten till skydd av personuppgifter, eftersom den gör det lättare för den registrerade att utöva andra rättigheter, t.ex. till korrigering och radering.

När det gäller rätten till korrigering och radering välkomnar arbetsgruppen att det har gjorts en avsevärd förbättring i skölden för skydd av privatlivet jämfört med safe harbour-principerna, eftersom det nu föreskrivs att dessa rättigheter inte enbart ska beviljas i situationer när uppgifterna är felaktiga utan även när uppgifter har behandlats i strid med principerna (bilaga II, II.6).

*2.2.6 Rättsmedel, genomförande och ansvar (prövningsmekanismer)*

a) Enskilda personer i EU ska kunna utöva rätten till prövning effektivt

Arbetsgruppen erkänner de amerikanska myndigheternas åtaganden när det gäller de olika nivåerna i prövningsmekanismen. Med tanke på komplexiteten och bristen på tydlighet i mekanismens allmänna utformning är arbetsgruppen emellertid rädd att de registrerades möjlighet att utöva sin rättighet i praktiken kommer att undergrävas. Arbetsgruppen påpekar att kvaliteten i prövningsmekanismen bör ha företräde framför kvantiteten mekanismer som enskilda personer i EU har tillgång till. Det finns också farhågor om att de flesta, om inte alla, prövningsmekanismer innebär ett förfarande i Förenta staterna, vilket gör det svårare för EU:s dataskyddsmyndigheter att övervaka förfarandet.

Den prövningsmekanism som föreskrivs i skölden för skydd av privatlivet är i själva verket främst inriktad på den registrerades möjlighet att ”utöva sina rättigheter och driva fall av bristande efterlevnad av principerna genom direkta kontakter med det självcertifierade företaget i Förenta staterna”[27]. Dessutom måste organisationer utse ett oberoende tvistlösningsorgan som ska utreda och lösa individuella klagomål. Arbetsgruppen välkomnar att detta ska anordnas utan kostnad för den enskilda personen.

Alternativt kan klagomål lämnas in direkt till en federala konkurrensmyndigheten (Federal Trade Commission, FTC), även om FTC inte är skyldig att hantera dem. En dataskyddsmyndighet kan också hänskjuta ett klagomål och det amerikanska handelsministeriet har åtagit sig att granska och göra sitt bästa för att underlätta lösningen av klagomål (bilaga I), och FTC kommer att ”prioritera” dem (bilaga II, III.7 e). Att FTC prioriterar klagomål garanterar dock inte att registrerades klagomål kommer att behandlas.

Som sista utväg kommer enskilda personer att kunna begära ett bindande skiljedomsförfarande. Skiljedomsarbetsgruppen ska baseras i Förenta staterna och granskas av amerikanska domstolar.

Enligt skölden för skydd av privatlivet får organisationen också välja att samarbeta med dataskyddsmyndigheterna i EU (bilaga II, III.5 a). Det är till och med obligatoriskt för personaluppgifter som har samlats in i samband med ett anställningsförhållande (bilaga II, III.9 d ii). I ett sådant scenario kommer alternativ tvistlösning inte att vara tillämplig (bilaga

[27] Europeiska kommissionens förslag till beslut om adekvat skyddsnivå, punkt 30.

II, III.5 a). Det fastställs inte tydligt i skölden för skydd av privatlivet hur samarbetet med dataskyddsmyndigheterna i EU ska organiseras i praktiken. Framför allt är det oklart om arbetsgruppen ska hantera samtliga ärenden eller om varje enskilt ärende ska hanteras av en annan arbetsgrupp.

Arbetsgruppen anser att det krävs närmare föreskrifter i beslutet om adekvat skyddsnivå i fråga om dataskyddsmyndigheternas befogenheter att hantera klagomål. Detta beror uppenbarligen på organisationens kvalifikationer, men det är oklart på vilket sätt.

Om organisationen agerar som förmedlare för en registeransvarig i EU kommer enskilda personer under alla omständigheter att kunna klaga hos den behöriga dataskyddsmyndigheten i EU. En liknande situation kommer att gälla för personalresurser och annan behandling av kommersiella uppgifter.

När den organisation som är ansluten till skölden för skydd av privatlivet agerar som registeransvarig kommer en dataskyddsmyndighet endast att ha befogenhet att hantera den del i klagomålet som gäller behandling som omfattas av EU-lagstiftningen (behandling under ansvar av den registeransvarige i EU – inklusive gemensamt ansvar tillsammans med den amerikanska organisationen – eller när den organisation som är ansluten till skölden direkt skulle omfattas av EU-lagstiftningen, t.ex. på grund av att den använder utrustning i EU). När behandlingen av uppgifter enbart omfattas av amerikansk lag kommer dock endast mekanismerna i skölden för skydd av privatlivet att vara tillämpliga. För att överbrygga språkbarriärer och bristande kunskaper om det amerikanska rättssystemet skulle det underlätta om EU:s dataskyddsmyndigheter fick rätt att agera som förmedlare av den enskilda personens klagomål eller att bistå honom eller henne i alternativa tvistlösningsförfaranden med amerikanska organisationer eller vid den berörda personens kontakter med de amerikanska myndigheterna, om dataskyddsmyndigheten anser att detta är lämpligt.

Arbetsgruppen betonar att den mekanism som beskrivs i skölden för skydd av privatlivet inte följer tidigare rekommendationer om att enskilda personer i EU bör ”kunna framställa krav på ersättning för skador i Europeiska unionen” och även ”ha rätt att lämna in klagomål hos en behörig nationell domstol i EU”[28]. Det vore bra om organisationer som är anslutna till skölden för skydd av privatlivet också tog med en sådan möjlighet i sina integritetspolicyer.

För att garantera att systemet blir effektivt rekommenderar arbetsgruppen att det ska vara möjligt för dataskyddsmyndigheter i EU att företräda den registrerade och agera på dennes vägnar eller fungera som mellanhand. Alternativt bör systemet omfatta särskilda jurisdiktionsklausuler som ger registrerade rätt att utöva sina rättigheter i EU.

b) Skiljedomsförfarande

De slutliga skiljedomsförfarandena är ännu inte klara, vilket försvårar arbetsgruppens bedömning. Eftersom det verkar som om systemet med skiljedomsförfarande ska omfattas av amerikansk lagstiftning och att engelska kommer att vara det enda språk som används vid

[28] Se arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014.

förfarandena, kan dataskyddsmyndigheterna i EU vilja ha befogenhet att bistå enskilda personer i förfarandet.

Dessutom har skiljedomsförfarandet införts på grund av att det inte fanns några garantier för att ett klagomål skulle behandlas, eftersom FTC inte har någon skyldighet att behandla varje klagomål. Om en enskild person i EU känner behov av bistånd från en jurist konstaterar arbetsgruppen att han eller hon måste täcka kostnaderna för det juridiska biståndet, vilket kan hindra enskilda personer från att lämna in sitt klagomål för ett skiljedomsförfarande.

c) Tillsyn, verkställighet och effektivitet i prövningsmekanismerna

Villkor för att få ansluta sig till skölden

Enligt EU-domstolen ”bygger ett [självcertifierings]systems tillförlitlighet […] i huvudsak på införandet av effektiva spårnings- och kontrollmekanismer som gör det praktiskt möjligt att upptäcka och beivra eventuella överträdelser av de bestämmelser som säkerställer skyddet av de grundläggande rättigheterna […].”[29]

Arbetsgruppen konstaterar att det amerikanska handelsministeriets roll i certifieringsförfarandet inom ramen för skölden för skydd av privatlivet verkar ha skurits ned till en kontroll av att dokumenten är fullständiga. Arbetsgruppen inser att självcertifiering inte innebär någon systematisk förhandskontroll av att integritetspolicyer tillämpas, men handelsministeriet bör åtminstone åta sig att göra systematiska kontroller av att integritetspolicyerna omfattar alla principer som ingår i skölden för skydd av privatlivet. Ett sådant åtagande nämns i förslaget till beslut om adekvat skyddsnivå, men framgår inte tydligt av handelsministeriets utfästelser.[30]

En överträdelse av principerna i skölden för skydd av privatlivet skulle fortgå obemärkt under lång tid och kanske inte bli upptäckt förrän den registrerades grundläggande rättigheter har skadats allvarligt, kanske rentav oåterkalleligt. Därför kan denna strategi strida mot EU:s försiktighetsprincip.

Insyn genom förteckningen över organisationer som är anslutna till skölden för skydd av privatlivet och ett register över organisationer som har tagits bort från den

Det har gjorts stora förbättringar när det gäller insyn för den registrerade. Utöver alla amerikanska organisationer som har självcertifierat sig hos handelsministeriet kommer den nya förteckningen också innehålla ett register över alla organisationer som har tagits bort från förteckningen över organisationer som är anslutna till skölden för skydd av privatlivet samt skälet till att en organisation har tagits bort.[31] Handelsministeriets webbplats för skölden för skydd av privatlivet kommer också att vara mer inriktad på målanvändarna för att underlätta kontrollen av vilken typ av information som omfattas av en organisations självcertifiering och

[29] EU-domstolen, Schremsmålet, punkt 81.
[30] Europeiska kommissionens förslag till beslut om adekvat skyddsnivå, punkt 34.
[31] Bilaga I, s. 5 och bilaga II, II.1. Arbetsgruppen hänvisar också till kommissionens fjärde rekommendation i meddelande COM(2103)847 och arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014, framför allt punkt 5 under ”Insyn”.

den integritetspolicy som gäller för den information som omfattas samt vilken metod som organisationen använder för att kontrollera att den följer principerna.[32] Arbetsgruppen välkomnar att det nu uttryckligen anges att handelsministeriet ska kontrollera att företag som har offentliga webbplatser offentliggör sin integritetsskyddspolicy där, eller, om de saknar offentlig webbplats, var integritetsskyddspolicyn har gjorts tillgänglig för allmänheten.[33] Dokumenten ger också mer information om integritetspolicyns innehåll.[34]

Arbetsgruppen anser att det skulle kunna uppstå problem om en organisation som redan ingår i förteckningen över organisationer som är anslutna till skölden för skydd av privatlivet i efterhand utökar sin certifiering till andra uppgiftskategorier. I sådana fall kommer förteckningen inte att återspegla principernas olika tillämpningsperioder för olika uppgiftskategorier. Detta innebär en risk för att enskilda personer och företag i EU inte fullt ut kan bedöma om en viss datamängd verkligen omfattas av principerna för skölden för skydd av privatlivet och, om så är fallet, från och med vilken tidpunkt. För att undvika denna brist rekommenderar arbetsgruppen att det ska anges separat för varje kategori av personuppgifter vilket datum självcertifieringen trädde i kraft för varje organisation som ingår i förteckningen över organisationer som är anslutna till skölden för skydd av privatlivet.

Arbetsgruppen välkomnar att det amerikanska handelsministeriet ska upprätthålla ett register över organisationer som har tagits bort från förteckningen över organisationer som är anslutna till skölden för skydd av privatlivet och att registret också ska innehålla ett förtydligande av orsaken till att dessa organisationer inte längre omfattas av fördelarna med skölden, och att organisationen måste fortsätta att tillämpa principerna på de personuppgifter som organisationen tog emot när den var ansluten till skölden, så länge den lagrar de uppgifterna (bilaga I, s. 3). Eftersom vissa organisationer som har tagits bort från förteckningen kan välja att lämna tillbaka eller radera uppgifter som de har tagit emot inom ramen för skölden för skydd av privatlivet, samtidigt som andra organisationer kommer att behålla uppgifter som de har tagit emot inom ramen för skölden, är det emellertid viktigt att ge enskilda personer större insyn i den här frågan. Därför bör det amerikanska handelsministeriets register över organisationer innehålla uppgifter om huruvida organisationen fortfarande har kvar uppgifter som har tagits emot inom ramen för skölden för skydd av privatlivet eller om den har lämnat tillbaka eller raderat de uppgifterna. Om organisationen fortfarande har kvar sådana uppgifter bör det i registret uttryckligen anges att organisationen måste fortsätta att tillämpa principerna på de uppgifterna.

Dessutom bör handelsministeriets register ange att dessa organisationer inte längre har rätt till de fördelar som skölden för skydd av privatlivet innebär för nya överföringar, vilket betyder att organisationen inte längre får ta emot personuppgifter från EU inom ramen för principerna.

[32] Bilaga I, s. 8. Arbetsgruppen hänvisar också till sin skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014, framför allt punkt 2 under ”Insyn”.
[33] Bilaga I, s. 3 och 4. Arbetsgruppen hänvisar också till kommissionens första rekommendation i meddelande COM(2103)847 och arbetsgruppens skrivelse till kommissionens vice ordförande Viviane Reding den 10 april 2014, framför allt punkt 3 under ”Insyn”.
[34] Bilaga I, s. 5 och 6 och bilaga II, III.6.

Kontrollförfaranden

För att kontrollera att självcertifieringen fungerar i praktiken kan organisationerna göra egenkontroller eller externa granskningar. Arbetsgruppen beklagar att det endast krävs utbildning för anställda när en organisation väljer att utföra kontrollen via egenkontroller (bilaga II, III.7 c). Dessutom verkar kontroller av att policyer är korrekta, heltäckande, offentliggjorda på ett tydligt sätt, tillämpas och är tillgängliga endast krävas om organisationen väljer intern granskning (egenkontroll) och kravet på externa granskningar begränsas till organisationens efterlevnad av integritetsskyddspolicyn.

Efterhandskontroll

Arbetsgruppen välkomnar att FTC och handelsministeriet har fått utredningsbefogenheter vid klagomål. Dessutom konstaterar arbetsgruppen att handelsministeriet kommer att kunna göra kontroller på eget initiativ, framför allt genom att skicka ut frågeformulär. Arbetsgruppen skulle dock ändå vilja förvissa sig om att denna metod räcker för att uppfylla EU-domstolens krav på effektiva mekanismer för att upptäcka och övervaka överträdelser. Arbetsgruppen undrar fortfarande exakt vilka befogenheter de amerikanska verkställande myndigheterna har för att göra inspektioner på plats hos självcertifierade organisationer för att utreda överträdelser av bestämmelserna i skölden för skydd av privatlivet, hur ett beslut som fattas av en myndighet i EU ska kunna få verkställighet på amerikanskt territorium och huruvida de påföljder som föreskrivs i skölden för skydd av privatlivet verkligen är avskräckande.

*2.2.7 Behandling av personaluppgifter*

Tillämpningsområde

Kompletterande princip 9 (bilaga II, III.9) ska tillämpas på personuppgifter om en (tidigare eller nuvarande) anställd som har samlats in i samband med anställningsförhållandet. Enligt formuleringen i kompletterande princip 9 a ii ska principerna för skölden för skydd av privatlivet endast tillämpas när ”identifierade [...] register överförs eller görs tillgängliga”. Begreppet ”identifierade register” stämmer inte överens med definitionen av ”personuppgifter” i bilaga II, I.8 a, som omfattar ”uppgifter om en identifierad eller identifierbar fysisk person” och är därför inte förenligt med den definition som används i direktivet[35].

I kompletterande princip 9 a ii anges följande: ”Statistikrapportering som bygger på sammanförda sysselsättningsuppgifter som inte innehåller personuppgifter eller användning av uppgifter som avidentifierats innebär inte något problem för integritetsskyddet.” Detta påstående står i strid med flera yttranden från arbetsgruppen. Arbetsgruppen vill betona att sammanförda uppgifter fortfarande kan återidentifieras och därmed bör betraktas som personuppgifter[36].

[35] Som arbetsgruppen redan har framhållit är inte heller begränsningen till register som ”överförs eller görs tillgängliga” förenlig med begreppet ”behandling” (bilaga II, I.8 b).
[36] Se yttrande 4/2007 om begreppet personuppgifter och yttrande 05/2014 om avidentifieringsmetoder.

Meddelande, valmöjlighet och ändamålsbegränsning

I kompletterande princip 9 b i finns ett exempel på tillämpning av principerna om meddelande och valmöjlighet, där personaluppgifter används för ett annat ändamål. Exemplet handlar om en amerikansk organisation som ”har för avsikt att använda personuppgifter som samlats in i samband med ett anställningsförhållande för marknadskommunikation”. Här är det tillåtet att ändra ändamålet, förutsatt att principen om meddelande och valmöjlighet tillämpas. Arbetsgruppen anser att vidare behandling av personaluppgifter för direktmarknadsföring i de flesta fall måste betraktas som ett oförenligt ändamål och därför stå i strid med principen om ändamålsbegränsning (bilaga II, II.5 a). Dessutom menar arbetsgruppen att valmöjlighet inte kan vara en lämplig grund för den anställdes ”samtycke” (opt-out) till en ändring av ändamålet när detta sker inom ramen för en anställning, där ett sådant samtycke kanske inte är helt och hållet fritt.

Arbetsgruppen tvivlar starkt på att sköldens starka inriktning på principen om valmöjlighet som ett villkor för vidare användning av uppgifter för ett annat ändamål uppfyller OECD:s riktlinjer för skydd av privatlivet, eftersom det saknas tillräckliga garantier för att förhindra att denna valmöjlighet också används för vidare behandling för oförenliga ändamål. I kompletterande princip 9 b iv medges uttryckligen ett brett undantag från principerna om meddelande och valmöjlighet ”[o]m och när det är nödvändigt att undvika inblandning i organisationens personalpolitik, dvs. befordringar, tillsättande av tjänster eller liknande”. För det första bör användningen av personaluppgifter för sådana ändamåls anges uttryckligen redan när uppgifterna samlas in. Dessutom är formuleringen ”eller liknande” för vag och omfattande. Detta kommer att leda till att personaluppgifter helt och hållet undantas från principen om meddelande och valmöjlighet när de behandlas inom ramen för anställningsförhållandet. Begreppet är så brett att det inte går att bedöma om vidare användning är förenlig med det ursprungliga ändamålet. Arbetsgruppen rekommenderar att detta undantag tas bort.

Rätt till tillgång

Enligt kompletterande princip 9 e i kan överföringar till en registeransvarig hos tredje part av personuppgifter för ett fåtal anställda ske vid tillfälliga anställningsbehov, såsom flyg- och hotellbokningar eller försäkringstäckning utan att principen om tillgång behöver tillämpas och utan att det är nödvändigt att ingå ett avtal med tredje partens personuppgiftsansvarige, på villkor att organisationen uppfyller principerna om meddelande och valmöjlighet. Arbetsgruppen kan inte se att det finns någon rimlig motivering för ett sådant undantag och rekommenderar att det här stycket raderas.

*2.2.8 Farmaceutiska och medicinska produkter*

Tillämpningsområde

Enligt skölden för skydd av privatlivet ska överföringar av kodade uppgifter från EU till Förenta staterna i samband med farmaceutiska och medicinska produkter inte betraktas som

överföringar som omfattas av skölden (bilaga II, III.14 g i). Överföring av kodade uppgifter omfattas emellertid av EU:s dataskyddslagstiftning. Det betyder att skölden för skydd av privatlivet inte kan omfatta sådana överföringar. Arbetsgruppen uppmanar kommissionen att uttryckligen ange att förslaget till beslut om adekvat skyddsnivå inte ska omfatta kodade uppgifter för farmaceutiska och medicinska ändamål och att sådana överföringar därför måste omfattas av andra garantier, t.ex. standardavtalsklausuler eller bindande företagsregler. Arbetsgruppen föreslår att detta ska förtydligas i det slutliga beslutet om adekvat skyddsnivå.

Överföringar för kontroll- och övervakningsändamål (bilaga II, III.14 d)

Arbetsgruppen är oroad över att personuppgifter, som för det mesta är känsliga på grund av det medicinska sammanhanget, kan överföras till tillsynsmyndigheter i Förenta staterna enligt dessa bestämmelser. Eftersom skölden för skydd av privatlivet är utformad för överföringar av uppgifter mellan privata enheter verkar ett offentligt organ, t.ex. en amerikansk tillsynsmyndighet, inte vara berättigat att göra en självcertifiering enligt skölden, vilket väcker frågan om huruvida uppgiftsskyddet är adekvat för sådana överföringar. Om sådana överföringar behöver utföras för tillsynsändamål måste det vidtas tillfredsställande åtgärder för att garantera ett kontinuerligt skydd av de grundläggande rättigheterna för registrerade i EU. Arbetsgruppen understryker att förslaget till beslut om adekvat skyddsnivå inte innehåller några slutsatser om detta. Därför har arbetsgruppen inga garantier för att känsliga uppgifter från registrerade i EU kommer att få ett adekvat skydd i detta sammanhang.

Dessutom förstår arbetsgruppen inte varför ändamålet ”marknadsföring” nämns som ett exempel på behandling för framtida vetenskaplig forskning. Det är också oklart varför vidare överföringar till produktionsanläggningar och övriga forskare (bilaga II, III.14 d) har placerats under rubriken ”Överföringar för tillsyns- och övervakningsändamål”. Dessa punkter måste förtydligas i det slutliga beslutet om adekvat skyddsnivå.

Produktsäkerhet och effektivitetskontroll (inklusive rapportering till statliga myndigheter) och spårande av patienter som använder vissa mediciner eller viss medicinsk utrustning

Enligt skölden för skydd av privatlivet går det att göra undantag från principerna om meddelande, valmöjlighet, vidare överföring och tillgång om anslutningen till principerna inverkar på efterlevnaden av lagstadgade krav. I förslaget till beslut om adekvat skyddsnivå finns inga slutsatser om situationer där principerna om skydd för privatlivet inverkar på efterlevnaden av lagstadgade krav. Arbetsgruppen kan visserligen förstå att statliga utredningar kan motivera begränsningar av rätten till meddelande och tillgång, för att skydda utredningarna, men kan inte se vilka skäl som skulle motivera så omfattande undantag när behandlingen utförs av organisationen eller av en tredje part inom den privata sektorn. Eftersom patienters behandlingar blir allt mer individualiserade är ett sådant brett undantag från principerna för skydd av privatlivet vid spårande av patienter som använder vissa mediciner eller viss medicinsk utrustning oacceptabelt, eftersom den här typen av vård kommer att vara vanligt förekommande. Detta gäller också när uppgifter används av läkemedelsföretag för övervakning av produktsäkerhet och effektivitetskontroll (prövning eller försäljning av nya läkemedel).

*2.2.9 Offentligt tillgänglig information*

Undantaget från rätten till tillgång när det gäller offentligt tillgänglig information och information i offentliga register (bilaga II, III.15 d och e) väcker farhågor om i vilken omfattning en enskild person när han eller hon utövar sin rätt till tillgång har intresse av att känna till att en viss registeransvarig behandlar uppgifter om honom eller henne, och också känna till vilka uppgifter som behandlas, för att kunna kontrollera behandlingen av sina uppgifter. Arbetsgruppen har vid upprepade tillfällen konstaterat att enligt EU-lagstiftningen har registrerade alltid rätt att få tillgång till sina uppgifter och vid behov kräva att uppgifterna korrigeras eller raderas, om de har behandlats på ett olagligt sätt eller om de är ofullständiga eller felaktiga, oavsett om personuppgifterna har offentliggjorts eller ej.[37] Om den enskilda personens begäran om tillgång avvisas på grund av att uppgifterna har hämtats från offentligt tillgängliga källor eller offentliga register skulle personen förlora sin möjlighet att kontrollera att uppgifterna är korrekta eller att de har offentliggjorts på ett lagenligt sätt över huvud taget.

I skölden för skydd av privatlivet undantas emellertid offentliga register och offentligt tillgänglig information från principerna om meddelande, valmöjlighet, tillgång samt ansvar för vidare överföringar (bilaga II, II.15 b). Dessa undantag verkar vara alltför omfattande jämfört med direktivet och väcker farhågor eftersom de bl.a. försämrar de enskilda personernas möjlighet att kontrollera att deras uppgifter är korrekta och att begränsa spridningen av deras uppgifter.

**2.3 Slutsatser**

Arbetsgruppen erkänner att de amerikanska myndigheterna och kommissionen har gjort stora förbättringar när det gäller de kommersiella aspekterna på överföring av uppgifter mellan de båda kontinenterna. Mot bakgrund av sin analys ovan konstaterar arbetsgruppen dock att den kommersiella delen av skölden för skydd av privatlivet behöver förtydligas ytterligare på många punkter. Bristen på en uttrycklig princip för lagring av uppgifter är t.ex. oroväckande. Därför tvivlar arbetsgruppen starkt på att skölden för skydd av privatlivet kan säkerställa en skyddsnivå som är väsentligen likvärdig med skyddet i EU.

Beslutet om adekvat skyddsnivå måste vara tydligare när det gäller principerna om ändamålsbegränsning och valmöjlighet. Risken för kryphål finns kvar i fråga om flera principer, framför allt när det gäller vidare överföringar, mekanismen för att hantera klagomål och behandling av personaluppgifter och farmaceutiska uppgifter. Hur principerna för skölden för skydd av privatlivet ska tillämpas på registerförare (förmedlare) behöver dessutom förtydligas ytterligare och uppmärksammas särskilt, för att se till att en tydlig och otvetydig terminologi tillämpas.

[37] Se WP20, s. 4.

# 3. BEDÖMNING AV GARANTIER SOM RÖR NATIONELL SÄKERHET I FÖRSLAGET TILL BESLUT OM ADEKVAT SKYDDSNIVÅ

## 3.1 Garantier och begränsningar som är tillämpliga för amerikanska nationella säkerhetsmyndigheter

Det kan vara tillåtet att inskränka de grundläggande rättigheterna till privatliv och uppgiftsskydd om detta är motiverat i ett demokratiskt samhälle. Detta betyder att principerna om skydd för privatlivet inte är absoluta och att det kan vara möjligt med undantag, men endast om de tillämpliga (grundläggande) garantierna uppfylls. Enligt målet om ökat integritetsskydd bör organisationerna dessutom sträva efter att genomföra principerna öppet och fullt ut, samt även ange i sina planer för integritetsskydd på vilka områden undantag från principerna enligt den amerikanska rättsliga ramen kommer att göras regelbundet. Av samma skäl förväntas organisationerna, såvida det finns en valmöjlighet enligt principerna och/eller amerikansk lag, välja en högre skyddsnivå om det är möjligt.

I bilaga II, I.5 anges att tillämpningen av principerna får begränsas ”a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller b) av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses, eller c) om följden av direktivet eller medlemsstaternas lagstiftning är att man tillåter undantag och avvikelser förutsatt att sådana undantag eller avvikelser tillämpas i jämförbara sammanhang.”

Frågan är om de undantag som anges i bilaga II är motiverade i ett demokratiskt samhälle. Enligt förslaget till beslut om adekvat skyddsnivå drog kommissionen slutsatsen att ”Förenta staterna har regler som är utformade för att se till att eventuella ingrepp av skäl som rör nationell säkerhet i de grundläggande rättigheterna för de personer vars personuppgifter överförs från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga”.[38]

Arbetsgruppen har använt den ram som anges i avsnitt 1.2 i det här yttrandet, de amerikanska myndigheternas skrivelser och kommissionens slutsatser för att bedöma den nuvarande amerikanska rättsliga ramen och praxis hos amerikanska underrättelsetjänster samt under vilka omständigheter de tillåter ingrepp i de grundläggande rättigheterna till respekt för privatlivet och uppgiftsskydd enligt EU:s rättsliga ram. Bedömningen baseras på en analys av Presidential Policy Directive 28 (PPD-28), Executive Order 12333 (EO12333) och de olika rättsliga grunder som har införts genom Foreign Intelligence Act (FISA – avsnitten 104, 402, 215, 501 och 702). Arbetsgruppen har utgått från bilaga VI till skölden för skydd av

[38] Kommissionens förslag till beslut enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom bestämmelserna om integritetsskydd mellan EU och Förenta staterna, punkt 75.

privatlivet, som omfattar en skrivelse från Office of the Director of National Intelligence (ODNI) om de garantier och begränsningar som är tillämpliga på Förenta staternas myndigheter för nationell säkerhet och med en sammanfattning av den information som kommissionen har fått om Förenta staternas signalspaning.

## 3.2 Garanti A – Behandlingen bör vara förenlig med lagstiftningen och baseras på tydliga, exakta och lättillgängliga regler

Enligt europeiska regler måste eventuella ingrepp göras i enlighet med lagar, etablerade policyer och förfaranden och vara tillräckligt tydliga och tillgängliga för att ge medborgarna en tillräcklig bild av under vilka omständigheter och på vilka villkor som offentliga myndigheter har rätt att vidta övervakningsåtgärder.[39]

Arbetsgruppen konstaterar att signalspaningen utförs på grundval av en tillgänglig rättslig ram. Alla lagar som anges i bilaga VI (PPD-28, FISA, USA FREEDOM ACT, FOIA) är tillgängliga för allmänheten online (i och utanför Förenta staterna). I bilaga VI finns en sammanfattning av den gällande rättsliga ramen, begränsningarna för insamling, lagring och spridning, efterlevnad och övervakning, insyn och prövning. Det amerikanska rättsliga systemet för underrättelseverksamhet består av flera olika dokument, däribland enskilda myndigheters rapporter, policyer och förfaranden, som måste analyseras om man ska få en bättre förståelse av hur verksamheten bedrivs såväl i teorin som i praktiken. Här har arbetsgruppen inriktat sig på ett begränsat antal punkter som den anser är avgörande.

### *3.2.1 Executive Order 12333 och Presidential Policy Directive 28*

EO12333 har stor räckvidd: i princip kan all utländsk underrättelseinsamling utföras efter Förenta staternas presidents skönsmässiga bedömning på grundval av denna order. Det har dock hävdats att EO12333 endast får användas för insamling av uppgifter utanför Förenta staternas territorium efter införandet av FISA. Arbetsgruppen konstaterar att EO12333 inte är särskilt detaljerad när det gäller dess geografiska räckvidd, i vilken omfattning uppgifter får samlas in, lagras eller spridas, eller vilken typ av överträdelser som kan leda till övervakning eller vilken typ av information som kan komma att samlas in eller användas.

Enligt arbetsgruppens uppfattning är det främsta syftet med Presidential Policy Directive 28 (PPD-28) att fastställa gränserna för insamling och behandling av personuppgifter oavsett vilket övervakningsprogram som används och var uppgifterna har kommit ifrån.

[39] Europadomstolen, Zakharovmålet, punkt 247: ”Domstolen har tidigare konstaterat att kravet på ’förutsägbarhet’ i lagen inte är så långtgående att staten är tvingad att införa rättsliga bestämmelser med detaljerade förteckningar över alla beteenden som kan leda till ett beslut om hemlig övervakning av en enskild person på grunder som rör ’nationell säkerhet’. Det ligger i sakens natur att hot mot den nationella säkerheten kan ha varierande egenskaper och vara oförutsedda eller svåra att definiera på förhand (se ovannämnda Kennedymål, punkt 159). Samtidigt har domstolen också betonat att i frågor som berör grundläggande rättigheter skulle det strida mot rättsstatsprincipen, som är en av de grundläggande principerna för ett demokratiskt samhälle och som fastställs i konventionen, om den verkställande makten ges obegränsat utrymme för eget skön inom området som rör den nationella säkerheten. Därför måste lagen fastställa räckvidden för ett eventuellt utrymme för eget skön som beviljas de behöriga myndigheterna samt hur det får utövas på ett tillräckligt tydligt sätt, med hänsyn till den berörda åtgärdens legitima syfte, så att den enskilda personen garanteras adekvat skydd mot godtyckliga ingrepp.”

PPD-28 är ett direktiv från Förenta staternas president om de principer för enhetlighet som ska tillämpas när signalspaning ska godkännas och utföras, men PPD-28 utgör inte någon rättslig grund för insamling. PPD-28 ger effekt genom att underrättelsemyndigheter åläggs att följa dess principer i sina policyer och förfaranden. Direktivet är tillämpligt på signalspaning oavsett var uppgifterna finns när de samlas in – i eller utanför Förenta staterna. Det gäller alltså också uppgifter som har samlats in för ändamål som rör signalspaning när de överförs från EU till Förenta staterna.

Framför allt anges i PPD-28 att signalspaning ska vara så skräddarsydd som möjligt[40]. När det gäller användning av uppgifterna fastställs förfaranden för uppgiftsminimering (inbegripet villkor för lagring och spridning av uppgifter), datasäkerhet och åtkomst för relevant personal (dvs. regler som innehåller garantier för att begränsa risken för missbruk och felaktig användning), uppgifternas kvalitet samt övervakning. Dessa garantier ska tillämpas oavsett vilken nationalitet de registrerade har, dvs. på medborgare i Förenta staterna och på medborgare i tredjeland.

De garantier som införs genom PPD-28 ska också tillämpas under överföringen av uppgifter till Förenta staterna. Bilaga VI innehåller ett åtagande från ODNI som innebär att om den amerikanska underrättelsegemenskapen skulle samla in uppgifter från transatlantiska kabelanslutningar ”skulle den göra detta enligt de begränsningar och garantier som anges häri, inklusive kraven i PPD-28”[41]. Arbetsgruppen konstaterar att det fortfarande saknas etablerad rättspraxis om huruvida det är lagligt att fånga upp information från kablar, oavsett vilket land som gör det. Förenta staterna varken bekräftar eller förnekar att de avlyssnar kabeltrafik för att samla in underrättelser.

Begreppet *signalspaning* definieras varken i PPD-28 eller i någon annan tillämplig text.

### *3.2.2 Foreign Intelligence Surveillance Act*

Rent generellt verkar texten till Foreign Intelligence Surveillance Act (FISA) vara mer tydlig och exakt. Tolkningen av många bestämmelser mot bakgrund av PPD-28 och därmed deras praktiska tillämpning beror dock till stor del på de olika myndigheterna. Det finns ännu ingen fullständig rapport om tillämpningen av de nya garantierna, men delegater från Förenta staterna har informerat företrädare för arbetsgruppen att garantierna i PPD-28 verkligen har genomförts fullt ut och tillämpas på ett likartat sätt i hela den amerikanska underrättelsegemenskapen.

Avsnitt 501 är förhållandevis tydligt när det gäller vilken typ av underrättelseverksamhet som kan tillåtas: ”alla konkreta föremål (inklusive böcker, register, skrivelser, dokument och andra föremål)”. Det bör dock påpekas att definitionen av *konkreta föremål* omfattar *andra föremål*, vilket innebär att befogenheten blir ganska omfattande.

[40] ”Signalspaning ska vara så skräddarsydd som möjlig. Vid beslut om signalspaning ska Förenta staterna ta hänsyn till tillgången till annan information, bl.a. från diplomatiska och offentliga källor. Sådana lämpliga och genomförbara alternativ till signalspaning bör prioriteras.” (Avsnitt 1 d.)

[41] Bilaga VI till skölden för skydd av privatlivet skrivelse från Office of the Director of National Intelligence (ODNI) om de garantier och begränsningar som är tillämpliga på Förenta staternas myndigheter för nationell säkerhet, s. 2.

Avsnitt 702, som innebär att uppgifter får samlas in om personer som inte är amerikanska medborgare och som skäligen kan antas befinna sig utanför Förenta staterna för att inhämta utländska underrättelseuppgifter[42], innehåller inte samma detaljerade föreskrifter som avsnitt 501. När det gäller räckvidden är avsnitt 702 inriktat på inhämtande av utländska underrättelser om enskilda personer utanför Förenta staterna med hjälp av amerikanska telekomtjänstleverantörer. Definitionen av *utländska underrättelseuppgifter* är bred. Den omfattar bl.a. ”uppgifter om en utländsk makt eller ett utländskt territorium som avser information som berör Förenta staternas utrikespolitik”[43], vilket skapar en viss osäkerhet om vilken typ av underrättelser som får samlas in i praktiken.

Trots att dokumenten inte längre är hemligstämplade är rapporterna till kongressen och övervakningsrapporterna från styrelsen för tillsyn av personlig integritet och medborgerliga friheter (Privacy and Civil Liberties Oversight Board, nedan kallad *PCLOB*), är tillämpningen av FISA, inklusive räckvidden för och användningen av de särskilda urvalstermerna, fortfarande otydlig och förvirrande. PCLOB hänvisar till användningen av särskilda urvalstermer (’avdelade urvalstermer’) i en rapport[44], men detta motsvarar inte de målsökningsregler som anges i avsnitt 702, enligt arbetsgruppens uppfattning[45]. De återges inte i allmänt tillgängliga bestämmelser enligt vad arbetsgruppen har kunnat finna.

### *3.2.3 Slutsats*

Överlag konstaterar arbetsgruppen att de tillämpliga texterna om underrättelseverksamhet är tillgängliga online och att de amerikanska myndigheterna har vidtagit ett antal viktiga åtgärder i fråga om öppenhet.

Arbetsgruppen erkänner att det sedan 2013 har offentliggjorts ett stort antal handlingar, såsom policyer, förfaranden, avgöranden i FISA-domsolen och andra beslut som inte längre är hemligstämplade. Dessutom har PCLOB offentliggjort viktiga rapporter om den verksamhet som bedrivs på grundval av avsnitt 702 och USA FREEDOM Act. En liknande rapport väntas om verksamhet som bedrivs på grundval av EO12333.

Flera lagstiftningsbilagor som hade kunnat belysa hur Executive Order påverkar enskilda personer utanför Förenta staterna och eventuella tillämpliga garantier är hemligstämplade och därför inte tillgängliga för allmänheten eller för de enskilda personer som eventuellt påverkas av deras tillämpning. De texter som inte längre är hemligstämplade har begränsat värde och ger endast begränsad insyn i underrättelseverksamheten.

Trots ansträngningarna för att förklara hur EO12333 fungerar efter Edward Snowdens avslöjanden och framför allt efter antagandet av PPD-28 är det fortfarande oklart hur EO12333 tillämpas i praktiken i dag. Arbetsgruppen konstaterar att bilaga VI till skölden för skydd av privatlivet inte innehåller några detaljerade uppgifter om hur EO12333 fungerar.

[42] 50 U.S. Code §1881a (D)(1).
[43] 50 U.S. Code § 1801 (e) (2).
[44] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, s. 32.
[45] 50 U.S. Code § 1881a(D).

Arbetsgruppen välkomnar de begränsningar som införs genom PPD-28, men det är svårt att avgöra om det amerikanska regelverket för övervakning är tillräckligt förutsägbart, dvs. ger ”tillräcklig indikation eller tillräckliga indikationer på under vilka omständigheter och på vilka villkor som offentliga myndigheter har befogenhet att vidta sådana åtgärder”, eftersom det ännu inte har gjorts några förtydliganden, t.ex. genom offentliggörandet av PCLOB:s rapport om EO12333.

## 3.3 Garanti B – Nödvändighet och proportionalitet med hänsyn till de legitima mål som eftersträvas måste påvisas

### *3.3.1 Presidential Policy Directive 28*

Genom Presidential Policy Directive 28 (PPD-28) infördes begränsningar ifråga om de ändamål för vilka personuppgifter får användas och de villkor på vilka de får lämnas ut. Detta påverkar insamlingen av signalspaningsuppgifter, oavsett vilken rättslig grund som används.

Framför allt anges i avsnitt 1 i PPD-28 att signalspaning alltid måste vara så skräddarsydd som möjligt. Detta är visserligen en begränsning, men det är svårt att avgöra om ”så skräddarsydd som möjligt” innebär att all uppgiftsinsamling är nödvändig och proportionerlig.

Enligt PPD-28 är det fortfarande tillåtet med bulkinsamling ”för att identifiera nya eller framväxande hot och annan viktig information som rör den nationella säkerheten och som ofta är gömd i de stora och komplexa systemen i den moderna globala kommunikationen”.[46] Arbetsgruppen konstaterar att enligt PPD-28 avses med ”*signalspaningsunderrättelser som samlas in i 'bulk'* den tillåtna insamling av stora mängder signalspaningsuppgifter som av tekniska eller operativa hänsyn förvärvas utan urvalsfaktorer (t.ex. specifika anläggningar, urvalstermer osv.)”.

Genom PPD-28 införs begränsningar för användningen av signalspaningsuppgifter som samlats in i bulk när det gäller syftet. De sex syften för vilka uppgifter får samlas in i bulk omfattar terroristbekämpning och andra former av allvarliga (transnationella) brott. Arbetsgruppens analys tyder på att ändamålsbegränsningen är ganska bred (eventuellt alltför bred) för att kallas målinriktad.

PPD-28 har inte avskaffat möjligheten till urskillningslös insamling av personuppgifter i bulk och omfattningen av dessa insamlingsmöjligheter är fortfarande oklar och kan vara stor. Här konstaterar arbetsgruppen att ODNI i bilaga VI bekräftar att ”all insamling i bulk av internetkommunikation som den amerikanska underrättelsegemenskapen utför genom

[46] Avsnitt 2 i PPD-28 och bilaga VI till skölden för skydd av privatlivet skrivelse från Office of the Director of National Intelligence (ODNI) om de garantier och begränsningar som är tillämpliga på Förenta staternas myndigheter för nationell säkerhet, s. 3.

signalspaning bedrivs inom en liten del av internet."[47] Arbetsgruppen skulle uppskatta att ytterligare belägg läggs fram för detta genom insynsåtgärder.

### *3.3.2 Foreign Intelligence Surveillance Act*

Minimeringsförfarandena i avsnitt 215 och avsnitt 702 i FISA infördes för att skydda amerikanska invånare från långtgående statlig tillgång till deras uppgifter. Dessa begränsningar är inte officiellt tillämpliga på utlänningar, även om amerikanska regeringstjänstemän vid ett flertal tillfällen i såväl officiella som privata möten med företrädare för arbetsgruppen har sagt att tillämpningsområdet för minimeringsförfarandena i praktiken har utvidgats till att omfatta alla personer, oavsett nationalitet eller bosättningsort.

I avsnitt 702 anges att inhämtande som har godkänts "ska utföras på ett sätt som är förenligt med det fjärde tillägget till Förenta staternas konstitution, som begränsar uppgiftsinsamling till vad som anses vara förenligt med principen om rannsakning på skälig grund. Här görs ingen åtskillnad mellan amerikanska företag och andra företag". Förutsatt att det fjärde tillägget tillämpas på alla uppgifter som samlas in i Förenta staterna skulle alltså bulkinsamling i Förenta staterna vara "oskälig" och strida mot konstitutionen.

Arbetsgruppen välkomnar slutsatsen i PCLOB:s rapport om att "i praktiken omfattas även personer som inte är amerikanska medborgare av de begränsningar för tillgång och lagring som krävs enligt de olika myndigheternas minimerings- och eller målinriktningsförfaranden, på grund av kostnaderna för och svårigheterna att identifiera och avlägsna uppgifter som berör amerikanska medborgare i en stor mängd uppgifter, vilket innebär att hela datamängden brukar behandlas i enlighet med de strängare amerikanska normerna".

Arbetsgruppen konstaterar också att enligt PCLOB:s slutsatser "genomförs programmet inte genom bulkinsamling av kommunikation". ODNI:s 2014 Statistical Transparency Report bekräftar denna slutsats. Enligt PCLOB:s rapport används dessutom "särskilda urvalsfaktorer", t.ex. en e-postadress eller ett telefonnummer för att målinrikta övervakningen.[48]

I motsvarande tillgängliga offentliga regler för målinriktning föreskrivs dock inga sådana målinriktade regler och deras enda syfte är att undvika målinriktning mot amerikanska medborgare eller personer som är etablerade i Förenta staterna. De fördelar som PCLOB menar att personer som inte är medborgare i Förenta staterna omfattas av i praktiken är dessutom inte rättsligt bindande eller fastställda i lagstiftningen, eftersom den tillgängliga lagstiftningen om målinriktning inte föreskriver sådana målinriktade regler och endast syftar till att undvika målinriktning mot amerikanska medborgare eller personer som är etablerade i Förenta staterna.

---

[47] Bilaga VI till skölden för skydd av privatlivet, skrivelse från Office of the Director of National Intelligence (ODNI) om de garantier och begränsningar som är tillämpliga på Förenta staternas myndigheter för nationell säkerhet, s. 4. Arbetsgruppen påminner i sammanhanget om rapporten om slutsatserna från EU:s medordförande i ad hoc-arbetsgruppen mellan EU och Förenta staterna om uppgiftsskydd, där det konstateras att "kommunikationsdata utgör en mycket liten andel av den globala internettrafiken", eftersom den "överväldigande majoriteten av den globala internettrafiken består av höga volymer strömning och nedladdningar, av t.ex. tv-serier, filmer och idrottsevenemang" (punkt 3.1.2 i rapporten)44.

[48] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, s. 32.

Dessutom påpekar arbetsgruppen att i den betydelse som används i avsnitt 702 avses med *personer* inte enbart enskilda personer utan också grupper, enheter, sammanslutningar, företag eller utländska makter. Att insamlingen motiveras med att ”ett väsentligt syfte för inhämtningen är att införskaffa utländska underrättelseuppgifter” lämnar också en viss osäkerhet när det gäller ändamål och nödvändighet. Arbetsgruppen välkomnar dock informationen i bilaga VI om att sammanlagt omkring 90 000 enskilda personer omfattades av målinriktning inom ramen för avsnitt 702 under 2014[49]. Den första översynen av skölden för skydd av privatlivet kommer att innebära en möjlighet att lägga fram ytterligare belägg för målinriktningsreglerna.

Hittills finns det ingen avgörande rättspraxis om huruvida det är lagligt med massiv och urskillningslös uppgiftsinsamling och efterföljande användning av personuppgifter för ändamål som rör brottsbekämpning, inklusive frågan om under vilka omständigheter sådan insamling och användning av personuppgifter får ske. EU-domstolen väntas ta upp denna fråga, åtminstone till viss del, under 2016, både i förenade målen Tele2 Sverige AB mot Post- och telestyrelsen och Secretary of State for the Home Department mot Davis m.fl.[50] och den rådgivning som ska lämnas om giltigheten i avtalet med Kanada om passageraruppgifter.[51] Arbetsgruppen påminner emellertid om att den konsekvent har ansett att massiv och urskillningslös uppgiftsinsamling inte under några omständigheter kan anses vara proportionerlig.[52]

### *3.3.3 Slutsats*

Trots de begränsningar som införts genom PPD-28 kvarstår arbetsgruppens farhågor, särskilt när det gäller proportionaliteten i uppgiftsinsamlingen. För det första finns det indikationer på att Förenta staterna forsätter sin massiva och urskillningslösa insamling av uppgifter, eller åtminstone inte utesluter att de fortfarande kan komma att göra detta i framtiden. Arbetsgruppen har alltid ansett att den typen av uppgiftsinsamling inte är förenlig med EU-lagstiftningen och därför inte är acceptabel.

För det andra konstaterar arbetsgruppen att målinriktad behandling av uppgifter eller behandling som är ”så skräddarsydd som möjligt” fortfarande kan betraktas som massiv. Om sådan massiv uppgiftsinsamling bör vara tillåten eller ej utreds för närvarande i förfaranden i EU-domstolen. Därför kommer arbetsgruppen inte att göra någon slutlig bedömning av lagligheten i målinriktad men massiv uppgiftsbehandling. Arbetsgruppen betonar dock att om målinriktad men massiv uppgiftsbehandling skulle tillåtas, bör principerna för målinriktning tillämpas både på insamlingen och på den efterföljande behandlingen av uppgifterna och kan inte begränsas till enbart användningen. Under alla omständigheter krävs det ett förtydligande av förslaget till beslut om adekvat skyddsnivå när det gäller de sex ändamål som anges i PPD-28 och för vilka uppgifter får samlas in ”i bulk”. I detta skede är arbetsgruppen inte övertygad

[49] Bilaga VI, s. 11.
[50] EU-domstolen, förenade målen C-203/15 och C-698/15.
[51] EU-domstolen, mål A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_sv.pdf

om att dessa ändamål är tillräckligt begränsade för att säkerställa att uppgiftsinsamlingen verkligen är begränsad till det som är nödvändigt och proportionerligt.

### 3.4 Garanti C – Det bör finnas en oberoende tillsyn

Förenta staterna har inte något gemensamt tillsynsorgan på federal nivå som övervakar underrättelse- och övervakningsprogrammens konsekvenser för privatlivet och uppgiftsskyddet. I stället omfattas den amerikanska underrättelseverksamheten av en tillsynsprocess i flera nivåer: det går att göra åtskillnad mellan intern och extern tillsyn. Arbetsgruppen erkänner att de amerikanska tillsynsorganens rapporteringspraxis är mycket detaljerad och till största delen offentlig.

#### *3.4.1 Intern tillsyn*

Alla underrättelse- och säkerhetsmyndigheter har anställda som ansvarar för att säkerställa efterlevnaden av den rättsliga ramen. Bl.a. annat finns generalinspektörer vars huvudsakliga uppgift är att bedöma myndighetens övergripande efterlevnad av lagstiftningen, däribland – men inte enbart – lagarna som berör integritets- och uppgiftsskydd. Generalinspektörerna utses enligt lag och ska (eller kommer snart att) utnämnas av presidenten och därefter bekräftas av senaten, för att se till att de är organisatoriskt oberoende och rapporterar till kongressen. Arbetsgruppen anser att generalinspektörerna därför sannolikt kommer att uppfylla kriteriet för organisatoriskt oberoende enligt EU-domstolens och Europadomstolens definition, åtminstone från och med att alla generalinspektörer har utsetts enligt det nya utnämningsförfarandet. För närvarande återstår vissa farhågor när det gäller generalinspektörer som har utsetts av direktören för den myndighet som de utövar tillsyn över.

Generalinspektörerna kan utfärda rekommendationer som sedan kan hänskjutas till justitiedepartementet och PCLOB eller till och med till det utskott i kongressen som kan verkställa rekommendationerna. Om generalinspektören upptäcker en överträdelse kan denna hanteras genom interna och politiska åtgärder och rapporteras till kongressen. Generalinspektören har t.ex. befogenhet att göra både revisioner och inspektioner.

Arbetsgruppen konstaterar att generalinspektörernas rapporter kan hållas hemliga för allmänheten och att en generalinspektör också kan hindras från att rapportera om de uppgifter som inspekteras är hemligstämplade. Rapporterna kommer dock alltid att omfattas av kongressens tillsyn, vilket är en grundläggande garanti, även om den inte ger grunder för enskild prövning.

Alla myndigheter har tjänstemän med ansvar för integritetsskydd och medborgerliga friheter som bistår i det obligatoriska egenrapporteringssystemet med tillsyn i kongressen.

Överlag kan de interna tillsynsmekanismerna sägas vara förhållandevis starka. För att motivera ingrepp i de grundläggande rättigheterna till integritets- och uppgiftsskydd måste tillsynen dock vara helt och hållet oberoende. Och även om arbetsgruppen respekterar och uppskattar det arbete som utförs av olika tjänstemän med ansvar för integritetsskydd och

medborgerliga friheter kan den inte dra slutsatsen att de har det oberoende som krävs för att agera som oberoende tillsynsorgan.

### *3.4.2 Extern tillsyn*

Den externa tillsynen består av ett antal olika mekanismer: rättslig tillsyn enligt avsnitt 501 och 702, som säkerställs av FISA-domstolen, tillsyn av kongressens utvalda underrättelseutskott samt de uppgifter som utförs av PCLOB.

Arbetsgruppen påminner om att tillsynen helst – vilket också konstateras av EU-domstolen och Europadomstolen – bör ligga hos en domare för att garantera att förfarandet utförs oberoende och opartiskt. Fram tills nyligen var förfarandet ensidigt, utan möjlighet för de berörda enskilda personerna att höras, eller ens få kännedom om ärendet. Även i dag är förfarandet i FISA-domstolen ensidigt, men efter antagandet av USA Freedom Act har det inrättats sakkunniga (amicus curiae) i FISA-domstolen. De sakkunniga agerar oberoende, men har inte utsetts för att försvara de enskilda personer som kan beröras av ärendet.

Genom USA Freedom Act bildades en grupp sakkunniga som skulle informera FISA-domstolen i viktiga ärenden. Domstolen valde ut fem advokater som har fått de säkerhetsklassificeringar som krävs och som ska ge teknisk rådgivning, närvara vid förhandlingar i FISA-domstolen och ta fram underlag, samt pröva sakfrågan i ett ärende sett ur ett integritets- och civilrättsperspektiv. De kommer dock bara att göra detta i viktiga ärenden eller när nya rättsliga frågor uppstår.[53]

Avdelning 215 omfattas nästan helt och hållet av rättslig tillsyn på förhand (men inte i efterhand) eftersom alla program som använder avsnitt 215 som grund för insamling måste godkännas av FISA-domstolen. I PCLOB-rapporten anges att ”avsnitt 702 skiljer sig från FISA:s traditionella ram för elektronisk övervakning både vad gäller de normer som tillämpas och avsaknaden av individualiserade avgöranden av FISA-domstolen. Enligt lagen ska justitieministern och chefen för den nationella underrättelsetjänsten göra årliga certifieringar för att godkänna målinriktningen mot icke amerikanska medborgare som skäligen kan antas befinna sig utanför Förenta staterna för att inhämta utländska underrättelseuppgifter utan att närmare ange för FISA-domstolen vilka personer som inte är amerikanska medborgare som kommer att omfattas av målinriktningen. […] Det finns inte heller något krav på att staten ska visa att det finns skälig grund för att anta att ett mål som omfattas av avsnitt 702 är en utländsk makt eller en agent för en utländsk makt, vilket krävs enligt de traditionella FISA-reglerna.”[54]

I kongressen utövar de utvalda underrättelseutskotten också tillsyn genom att godkänna underrättelseverksamhet, framför allt genom att rösta om budgeten. Underrättelseutskotten i senaten och representanthuset får hemligstämplad information om underrättelseverksamheten. Justitieministern måste rapportera varje halvår till dessa utskott om FISA:s elektroniska

[53] Freedom Act TITLE IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS Sec. 401. Utnämning av sakkunniga.
[54] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, s. 24 och 25.

övervakning. Arbetsgruppen har ännu inte fått klart för sig i vilken omfattning de kan diskutera behandlingen av enskilda personers personuppgifter, särskilt när det gäller personer som inte är amerikanska medborgare.

PCLOB är en oberoende del av den verkställande grenen i den amerikanska förvaltningen och har två grundläggande befogenheter: 1) att granska och analysera de åtgärder som den verkställande grenen vidtar för att skydda [den amerikanska] nationen från terrorism, säkerställa att behovet av sådana åtgärder vägs mot behovet av att skydda integriteten och de medborgerliga friheterna, och 2) att säkerställa att farhågor i fråga om friheten behandlas på ett lämpligt sätt i utvecklingen och tillämpningen av lagar, föreskrifter och policyer som berör ansträngningar för att skydda nationen mot terrorism. Arbetsgruppen konstaterar att PCLOB har befogenhet att utfärda förelägganden och få tillgång till hemligstämplad information. Samtidigt som PCLOB utför sina uppgifter kontrollerar den också om programmen är effektiva. Den utövar inte tillsyn före, utan efter fullbordat faktum. PCLOB har visat sitt oberoende genom att vara oense med Förenta staternas president i rättsliga frågor. Framför allt konstaterade styrelsen att programmet för telefonmetadata inom ramen för avsnitt 2015 inte hade godkänts rättsligt och att det inte fanns några belägg för att det förhindrade attacker. PCLOB gjorde också en årslång undersökning av 702-programmet och konstaterade att det är lagligt och tydligt godkänt enligt lag, samt att avsnitt 702 har visat sig vara mycket effektivt, även när det gäller terrorism. Slutligen vidtog den åtgärder i fråga om kravet på insyn och konstaterade att ett antal hemligstämplade fakta inte behövde vara hemliga. PCLOB väntas rapportera om genomförandet av PPD-28 inom den närmaste framtiden. Här anser styrelsen att lagring av uppgifter om en utlänning enbart på grund av att personen är utlänning inte räcker.

Slutligen konstaterar arbetsgruppen att EO12333 inte innehåller några föreskrifter om domstolsprövning, tillsyns- eller prövningsmekanismer för övervakningsprogram som genomförs på dess grund.

### *3.4.3 Slutsats*

Förslaget till beslut om adekvat skyddsnivå visar att Förenta staterna har en strategi i flera nivåer för såväl intern som extern tillsyn. Tillsynsmekanismernas funktion kan vara förvirrande, men arbetsgruppen konstaterar att det rent allmänt finns tillräckliga interna tillsynsmekanismer. Däremot är arbetsgruppen oroad över att tillsynen över de övervakningsprogram som genomförs på grundval av EO12333 inte är tillräcklig.

Arbetsgruppen konstaterar att dess tidigare kritik av att förfarandena i FISA-domstolen inte är kontradiktoriska har avhjälpts till viss del genom att det har inrättats sakkunniga som har i uppgift att ”öka skyddet av enskilda personers integritet och medborgerliga friheter”. Trots detta utövar FISA-domstolen inte någon effektiv rättslig tillsyn över målinriktningen mot personer som inte är amerikanska medborgare. Det kvarstår också vissa tvivel på FISA-

domstolens förmåga att göra en effektiv bedömning av målinriktnings- och minimeringsförfarandena, vilket också konstaterades av PCLOB.[55]

## 3.5 Garanti D – Den enskilda personen måste ha tillgång till effektiva rättsmedel

### *3.5.1 Rättsmedel*

#### *3.5.1.1 Kravet på grund för att väcka talan*

Det amerikanska systemet för rättsmedel har en viktig begränsning: enligt den amerikanska konstitutionen måste den enskilda personen visa att den har grund för att väcka talan: ”kravet på att klagande har lidit eller kommer att lida direkt skada och att denna skada går att gottgöra. På federal nivå kan rättsliga åtgärder inte vidtas enbart på den grunden att en enskild person eller en grupp är missnöjd med en statlig åtgärd eller lag.”[56] Detta krav verkar sakna betydelse, eftersom enskilda personer inte meddelas om övervakningen ens när åtgärderna har avslutats. EU-domstolen och Europadomstolen har flera gånger konstaterat att enskilda personer måste ha tillgång till administrativ eller rättslig prövning. Europadomstolen bekräftade i sitt avgörande i Zakharovmålet att enligt domstolens rättspraxis kan var och en som har legitima skäl att misstänka ett ingrepp i sina grundläggande rättigheter får vända sig till domstol.[57]

Dessutom har utländska medborgare som befinner sig utanför Förenta staterna inte fullt konstitutionellt skydd i Förenta staterna, enligt rättspraxis från Förenta staternas högsta domstol[58]. Detta gäller framför allt i förhållande till det fjärde tillägget, som skyddar amerikanska medborgare – men inte personer som inte är amerikanska medborgare – mot rannsakningar och beslag på oskälig grund, och från vilket en stor del av den amerikanska rätten till integritet härleds. Medborgare i europeiska länder och andra européer som bor utanför Förenta staterna är helt enkelt uteslutna från det skydd som det fjärde tillägget innebär.[59]

Den begränsade tillämpningen av Judicial Redress Act (både vad gäller innehållet, eftersom den utesluter nationell säkerhet, men också i fråga om vilka personer som kan åberopa lagen), de många undantagen och den rättsliga osäkerheten om vilka myndigheter som lagen kommer att vara tillämplig på innebär att kravet på effektiva rättsmedel för alla enskilda personer som berörs av övervakningsärenden som rör nationell säkerhet inte uppfylls.

#### *3.5.1.2 Presidential Policy Directive 28*

Arbetsgruppen konstaterar att PPD-28 endast är ett direktiv och därför inte kan skapa några rättigheter för enskilda personer. Det kan bara göras genom lagstiftning. Därför kan enskilda

[55] PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, s. 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing, Clapper mot Amnesty International USA.
[57] Europadomstolen, Zakharovmålet, punkt 171.
[58] Förenta staterna mot Verdugo – Urquidez , s. 264–266.
[59] Rapport från EU:s medordförande, avsnitt 2.

personer inte vända sig till domstol på grundval av en påstådd överträdelse av garantierna i PPD-28.

*3.5.1,3 Foreign Intelligence Surveillance Act*

Enligt FISA finns det vissa prövningsmöjligheter för enskilda personer vid olaglig övervakning. Enligt FISA ”ska en förfördelad person, som inte är en utländsk makt eller en agent för en utländsk makt [...] som har blivit föremål för elektronisk övervakning eller om vilken uppgifter som har inhämtats genom elektronisk övervakning av den personen har lämnats ut eller använts i strid med avsnitt 1809 i denna avdelning ha grund för att väcka talan mot den person som har begått denna överträdelse”. Detta utesluter emellertid uttryckligen den utländska makt eller agent för en utländsk makt som var föremål för åtgärden. Den klagande måste dessutom som sagt visa att den har grund för att väcka talan, vilket inte kommer att vara möjligt i praktiken.

Genom USA Freedom Act har det inrättats en rådgivande arbetsgrupp av sakkunniga (amicus curiae) för FISA-domstolen som ska ge (frivillig) rådgivning vid viktig ny rättslig tolkning. Deras uppgift är emellertid att lämna opartiska råd och inte att försvara intressena hos en viss enskild person på dennes begäran.

*3.5.2 Administrativa prövningsmöjligheter*

*3.5.2.1 Generalinspektörer*

En annan möjlighet till prövning är att gå via generalinspektören, som det går att lämna in klagomål hos. Generalinspektörerna är dock inte skyldiga att behandla varje enskilt klagomål: man har inte rätt att att bli hörd, utan generalinspektörerna får besluta om behandling efter eget skön. Generalinspektören kan också utfärda rapporter med slutsatser om överträdelser där informationen inte längre är hemligstämplad. Om en enskild person kan anta att rapporten påverkar honom eller henne skulle han eller hon kunna vända sig till en domstol på grundval av den konstaterade överträdelsen av lagen.

*3.5.2.2 Freedom of Information Act*

Ett rättsmedel som är tillgängligt för alla är möjligheten att lämna in en begäran om tillgång till handlingar utifrån Freedom of Information Act (FOIA). Enligt de amerikanska myndigheterna kan vem som helst göra en FOIA-ansökan – oavsett om man är amerikansk medborgare eller ej – genom att helt enkelt begära ut uppgifter från en myndighet. Detta omfattar uppgifter om den enskilda personen, även om det i sådant fall krävs att man kan bevisa sin identitet. Om informationen är hemligstämplad för att skydda den nationella säkerheten är det dock osannolikt att en FOIA-ansökan kommer att godkännas, eftersom det finns ett undantag: myndigheterna är inte skyldiga att ge tillgång till hemligstämplade uppgifter, inte ens om uppgifterna avser den person som lämnade in ansökan. Uppgifter från pågående brottsutredningar är helt och hållet undantagna från FOIA-ansökningar. Såvitt arbetsgruppen förstår innebär FOIA-ansökan inte någon rätt att få lagligheten i uppgiftsbehandlingen prövad av en oberoende myndighet.

### *3.5.3 Ombudsman för skölden för skydd av privatlivet*

#### *3.5.3.1 Inrättande av en ombudsman*

I skölden för skydd av privatlivet införs en ny mekanism för att ”enskilda personer i EU” ska kunna lämna in förfrågningar om ”Förenta staternas signalspaning” till den nyinrättade ombudsmannen för skölden för skydd av privatlivet. Undersekreterare Catherine A. Novelli kommer att utses till ombudsman enligt det memorandum som bifogas skrivelsen från utrikesminister John Kerry av den 22 februari 2016. Hon kommer att ha denna funktion utöver sin roll som ”chefssamordnare för internationell it-diplomati”, som inrättas i avsnitt 4 d i PPD-28. I skrivelsen och i memorandumet betonas att undersekreteraren ska rapportera direkt till utrikesministern och är oberoende av underrättelsegemenskapen.

Trots namnet, fastställs i memorandumet att ombudsmannen för skölden för skydd av privatlivet inte enbart kommer att hantera förfrågningar om ärenden som handlar om tillgång till uppgifter som överförts från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet rörande nationell säkerhet, utan också om ärenden som rör standardavtalsklausuler, bindande företagsregler samt undantag (enligt artikel 26 i direktiv 95/46/EG) eller ”möjliga framtida undantag”, i enlighet med definitionen i fotnot 2 till memorandumet.

Hur mekanismen är tänkt att fungera kan sammanfattas på följande sätt: En enskild person i EU lämnar in en förfrågan till en behörig myndighet för tillsyn över nationella säkerhetstjänster i en medlemsstat eller till ett centraliserat ”organ som handlägger klagomål från enskilda personer i EU”, vilket i så fall kommer att inrättas eller utses. Den myndighet som förmedlar förfrågan till ombudsmannen måste först kontrollera att förfrågan är fullständig i enlighet med punkt 3 b i skrivelsen.[60] När förfrågan har skickats vidare till ombudsmannen för skölden för skydd av privatlivet och det har fastställts att den är förenlig med punkt 3 b ska ombudsmannen besvara förfrågan. Detta innebär att ombudsmannen slutligen ska bekräfta att ”i) klagomålet har blivit ordentligt utrett och att ii) Förenta staternas relevanta lagstiftning – inklusive i synnerhet de begränsningar och garantier som anges i skrivelsen från Office of the Director of National Intelligence (ODNI) – har följts eller, vid bristande efterlevnad, sådana brister har åtgärdats.”[61] Svaret kommer ”varken att bekräfta eller förneka om den enskilda personen har varit föremål för övervakning eller ange vilka

[60] b) EU-organet för handläggning av klagomål kommer att vidta följande åtgärder för att kontrollera att förfrågningarna är fullständiga:
i) Kontrollera den enskilda personens identitet och att personen agerar för egen räkning och inte som företrädare för en statlig eller mellanstatlig organisation.
ii) Se till att förfrågningar görs skriftligen och att de innehåller följande grundläggande information:
• All information som ligger till grund för förfrågan.
• Typ av information eller upprättelse som söks.
• De statliga organ i Förenta staterna som anses vara delaktiga, om några.
• Andra åtgärder som vidtagits för att erhålla den begärda informationen eller upprättelsen och de svar som mottagits till följd av dessa andra åtgärder.
iii) Kontrollera att förfrågan avser uppgifter som skäligen kan anses ha överförts från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet eller enligt standardavtalsklausuler, bindande företagsregler, undantag eller möjliga framtida undantag.
iv) Fastställa att förfrågan inte är oseriös eller görs av okynne eller i ond tro.

[61] Skölden för skydd av privatlivet, bilaga III avsnitt 4 e.

specifika avhjälpande åtgärder som har vidtagits".[62] När det gäller frågan om hur ombudsmannens utredning ska utföras, förklaras att ombudsmannen för skölden för skydd av privatlivet kommer att "föra ett nära samarbete med andra tjänstemän i den amerikanska regeringen, inbegripet lämpliga oberoende tillsynsorgan"[63]. Ombudsmannen kommer att "nära samordna arbetet med den nationella underrättelsetjänsten (Office of the Director of National Intelligence, ODNI), justitieministeriet och i förekommande fall andra berörda ministerier och myndigheter när det gäller Förenta staternas nationella säkerhet samt generalinspektörer och tjänstemän som ansvarar för lagen om informationsfrihet, medborgerliga friheter och integritetsskydd"[64]. Samordningen ska göras på ett sätt som säkerställer att ombudsmannen för skölden för skydd av privatlivet kan svara och ge de bekräftelser som beskrivs ovan.

*3.5.3.2 Bedömning av den nya ombudsmansmekanismen*

Arbetsgruppen erkänner kommissionens och den amerikanska regeringens ansträngningar för att införa en ny mekanism som syftar till att förbättra möjligheterna till rättslig prövning av amerikansk övervakningsverksamhet. Arbetsgruppen förstår att bedömningen av denna mekanism är särskilt viktig, eftersom detta är ett nytt inslag i de internationella förbindelserna i fråga om signalspaning och nationell säkerhet.

I det här avsnittet kommer arbetsgruppen att bedöma hur inrättandet av en ombudsman för skölden för skydd av privatlivet påverkar de nödvändiga kraven på att enskilda personer ska kunna söka rättslig prövning i enlighet med stadgan, Europakonventionen och de europeiska domstolarnas rättspraxis.

*3.5.3.3 Kan inrättandet av ombudsmannen i sig vara tillräckligt?*

Till att börja med måste man fråga sig om inrättandet av en "ombudsman" någonsin kan anses vara förenligt med artikel 47 i stadgan – där det föreskrivs ett effektivt rättsmedel inför en opartisk domstol[65] – åtminstone om det inte finns något annat sätt att söka en effektiv rättslig prövning. Detta är viktigt eftersom EU-domstolen i Schremsmålet, i den viktiga punkten 95, hänvisar till artikel 47 i stadgan, utan att ge några indikationer på att artikel 47 ska tolkas annorlunda i samband med övervakningsverksamhet. Tvärtom tillämpade EU-domstolen artikel 47 i stadgan redan i Kadi II-målet[66] på övervakningsverksamhet som berörde nationell respektive internationell säkerhet[67].

[62] Skölden för skydd av privatlivet, bilaga III avsnitt 4 e.
[63] Skölden för skydd av privatlivet, bilaga III avsnitt 2 a.
[64] Skölden för skydd av privatlivet, bilaga III avsnitt 2 a.
[65] I Förklaring avseende stadgan om de grundläggande rättigheterna konstaterade domstolen dessutom att artikel 47 garanterar rätten till ett effektivt rättsmedel inför en domstol (Förklaring avseende stadgan om de grundläggande rättigheterna, Förklaring till artikel 47 (2007/C 303/02).
[66] Domstolens dom den 18 juli 2013, Europeiska kommissionen och Förenade kungariket/Kadi, förenade målen C-584/10 P, C-593/10 P och C-595/10 P, ECLI:EU:C:2013:518.
[67] Kadi II-målet, punkterna 97 och 100: unionsdomstolarna kontrollerar lagenligheten hos alla unionsrättsakter, även rättsakter vilka syftar till att genomföra resolutioner som antagits av säkerhetsrådet med stöd av kapitel VII i Förenta nationernas stadga (kapitel VII handlar om hot mot freden, fredsbrott och angreppshandlingar).

Av Europadomstolens rättspraxis framgår det dock mycket tydligt att möjlighet till rättslig prövning i vanlig domstol inte är ett villkor för att övervakningsprogram ska anses vara förenliga med artikel 8 (och artikel 13 i Europakonventionen).[68] Snarare har domstolens praxis enligt artikel 8 blivit att det kan vara lämpligt med prövning hos andra myndigheter, som en nödvändig garanti vid övervakningsverksamhet. Europadomstolen ställer emellertid höga krav på att andra myndigheter ger möjlighet till effektiv prövning och konstaterar att sådana myndigheter måste vara ”oberoende av de myndigheter som utför övervakningen och ha tillräckliga befogenheter och tillräcklig kompetens för att utöva en effektiv och kontinuerlig kontroll”[69].

I Kennedymålet och i Klassmålet förklarade Europadomstolen vad dessa förväntningar kan innebära i samband med hemlig övervakning, när den registrerade inte meddelas om att hans eller hennes uppgifter behandlas. I båda dessa domar ansåg Europadomstolen att myndigheterna var oberoende. De var framför allt oberoende av de organ som utförde övervakningen, men även oberoende av instruktioner[70] från någon annan myndighet. I Kennedymålet godkände domstolen en oberoende och opartisk myndighet som hade antagit sin egen arbetsordning och som bestod av medlemmar som hade eller hade haft högt uppsatta tjänster inom rättsväsendet eller som var erfarna advokater[71].

När de myndigheter som berörs i de båda domarna åtog sig att granska klagomål från enskilda personer hade de tillgång till all relevant information, inbegripet hemligstämplat material. Slutligen hade båda befogenheter att åtgärda bristande efterlevnad.[72]

Utöver frågan om huruvida ombudsmannen kan betraktas som en ”domstol” innebär tillämpningen av artikel 47.2 i stadgan ytterligare en utmaning eftersom den föreskriver att domstolen måste ha ”inrättats enligt lag”. Det är tveksamt om ett memorandum med en beskrivning av funktionen hos en ny mekanism kan betraktas som ”lag”.

I stället för att bedöma om en ombudsman formellt kan betraktas som en domstol som har inrättats enligt lag beslutade arbetsgruppen därför – med väsentlig likvärdighet i åtanke – att arbeta vidare med de olika nyanserna i rättspraxis i fråga om de särskilda krav som är nödvändiga för att ”rättsmedel” och ”rättslig prövning” ska anses uppfylla de grundläggande rättigheter som fastställs i artiklarna 7, 8 och 47 i stadgan och artikel 8 (och 13) i Europakonventionen. I sin fortsatta analys kommer arbetsgruppen i sin diskussion av den nya mekanismens tillämpningsområde därför att inrikta sig på följande kriterier: kravet på att en förfrågan ska lämnas in till ombudsmannen och att förfrågan ska besvaras (”grund för att väcka talan”), ombudsmannens oberoende samt hans/hennes utredningsbefogenheter när det gäller att få tillgång till nödvändigt material, däribland hemligstämplade handlingar, liksom

[68] Enligt artikel 13 i Europakonventionen är medlemsländerna skyldiga att se till att ”[v]ar och en, vars (...) fri- och rättigheter kränkts, skall ha tillgång till ett effektivt rättsmedel inför en nationell myndighet”. Detta måste inte nödvändigtvis vara en rättslig myndighet, vilket Europadomstolen förtydligade i Klassmålet, punkterna 56 och 67.
69 Klassmålet, punkterna 56 och 67.
[70] Europadomstolen, Klassmålet, punkterna 21 och 53.
[71] G10-kommissionen består (när domen antogs) av tre medlemmar, varav ordföranden måste vara kvalificerad att inneha en befattning inom rättsväsendet, Klassmålet, punkterna 21 och 53).
[72] Europadomstolen, Kennedymålet, punkt 167 och Klassmålet, punkterna 21 och 53.

att begära bistånd från andra myndigheter och, slutligen, ombudsmannens befogenhet att åtgärda bristande efterlevnad.

*3.5.3.4 Ombudsmansmekanismens tillämpningsområde*

När det gäller tillgången till ombudsmansmekanismen anser arbetsgruppen att alla personer som omfattas av EU-lagstiftningen bör omfattas av de garantier som ingår i skölden för skydd av privatlivet. Det skulle inte vara acceptabelt att göra åtskillnad baserad på nationalitet, framför allt inte eftersom de grundläggande rättigheterna i EU är tillämpliga på alla och inte enbart på dem som har ett EU-pass. I bilaga III hänvisas till ”enskilda personer i EU” utan någon ytterligare definition av vad som avses. Arbetsgruppen beklagar denna osäkerhet och föreslår att det ska göras ett förtydligande om att alla personer som omfattas av EU-lagstiftningen har rätt att få sin förfrågan hos ombudsmannen behandlad i enlighet med villkoren i memorandumet. Dessutom bör kommissionen och Förenta staterna ta upp frågan om i vilken omfattning skölden för skydd av privatlivet också ska tillämpas på medborgare/invånare i EES-länderna och Schweiz, som tidigare faktiskt omfattades av safe harbour-systemet.

Arbetsgruppen konstaterar också att det råder viss osäkerhet i fråga om ombudsmansmekanismens tillämpningsområde. I memorandumet anges att ombudsmannen ska ansvara för att behandla förfrågningar som handlar om uppgifter som överförts från EU till Förenta staterna rörande nationell säkerhet i enlighet med alla överföringsverktyg som är tillgängliga enligt EU-lagstiftningen, men det framgår också tydligt av memorandumet att detta är en mekanism som avser ”signalspaning”. Det senare begreppet tyder på att det endast är överföringar av uppgifter som har samlats in genom signalspaning som omfattas, vilket väcker frågan om huruvida uppgifter som har samlats in i enlighet med FISA t.ex. ska betraktas som ”signalspaning”. Detta verkar vara fallet i fråga om avsnitt 702, vilket förklaras i ODNI:s utfästelser, s. 10.[73] Arbetsgruppen beklagar dock att användningen av begreppet ”signalspaning” skapar onödig osäkerhet i det här sammanhanget.

Såvitt arbetsgruppen förstår kommer ombudsmansmekanismen inte heller att täcka åtföljande förfrågningar om tillgång för brottsbekämpande myndigheter.[74] I så fall är det fortfarande oklart om förfrågningar från vissa myndigheter, framför allt CIA, skulle omfattas av mekanismen.

*3.5.3.5 ”Grund för att väcka talan” och förfarandet för förfrågan*

Det är mycket svårt att inleda rättsliga förfaranden mot Förenta staternas övervakningsverksamhet inför vanliga domstolar i Förenta staterna. Arbetsgruppen är medveten om att högsta domstolen har vägrat talesrätt i underrättelseärenden där den sökande inte har kunnat bevisa individuell ”konkret, exakt och faktisk eller nära förestående skada”.[75] I detta avseende är inrättandet av en ombudsman ett viktigt steg eftersom det ger en extra

[73] Skölden för skydd av privatlivet, bilaga VI, s. 10.
[74] Memorandum om inrättande av en ombudsman, s. 1.
[75] Clapper mot Amnesty International USA, 568 U.S. ___ (2013) II. s. 10.

möjlighet att få någon form av rättslig prövning som annars inte skulle finnas. Därför välkomnar arbetsgruppen förtydligandet i avsnitt 3 c. Enligt detta avsnitt är det inte nödvändigt att bevisa att den sökandes uppgifter verkligen har gjorts tillgängliga genom signalspaning för att lämna in en förfrågan inom ramen för den nya mekanismen.

Arbetsgruppen ställer sig i stort sett bakom förfarandet för att identifiera den klagande inom ramen för ombudsmansmekanismen. Det är fullt rimligt att identifieringen ska ske inom EU:s territorium, vilket också är fallet för tillgångsmekanismen inom ramen för TFTP2-avtalet mellan EU och Förenta staterna. Däremot kan arbetsgruppen inte förstå varför kontrollen i EU ska utföras av ”medlemsstaternas tillsynsmyndigheter med behörighet för tillsyn över nationella säkerhetstjänster”. Med hänsyn till artikel 4.2 i Fördraget om Europeiska unionen verkar det för det första osannolikt att kommissionen kan ålägga dessa myndigheter att utföra uppgifter, eftersom de uppenbart omfattas av medlemsstaternas behörighet.

Med tanke på hur olika tillsynsmekanismerna för nationella säkerhetstjänster fungerar i medlemsstaterna kan motsvarande myndigheters delaktighet dessutom påverka systemets effektivitet kraftigt för invånarna i medlemsstaterna. Det kan t.ex. handla om fall där flera myndigheter har ansvar för tillsynen över de nationella säkerhetstjänsterna och det kan vara svårt för den enskilda personen att identifiera vilken myndighet som är relevant, fall där de tillämpliga nationella rättsliga reglerna inte innehåller några bestämmelser om enskilda personers möjlighet att ta kontakt med relevant tillsynsmyndighet, eller fall där dessa myndigheter inte har inrättats på ett sådant sätt att de kan utföra de uppgifter som de åläggs enligt förslaget till beslut om adekvat skyddsnivå[76]. Eftersom dataskyddsmyndigheterna deltar i tillämpningen och övervakningen av skölden för skydd av privatlivet och har en liknande roll inom ramen för TFTP2-avtalet verkar det mer förnuftigt att lägga denna uppgift på medlemsstaternas nationella dataskyddsmyndigheter. Arbetsgruppen understryker att den anser att det är osannolikt att hemligstämplad information kommer att behandlas inom ramen för ett förfarande hos ombudsmannen för skölden för skydd av privatlivet, eftersom svaret endast kommer att bli ”följer bestämmelserna, eller följer inte bestämmelserna men har åtgärdats”.

*3.5.3.6 Oberoende*

Av utrikesministerns utfästelser framgår tydligt att ombudsmannens roll ska fyllas av en undersekreterare vid utrikesministeriet. Denna utnämns av presidenten och måste godkännas av senaten. Rollen som ombudsman kräver inte något ytterligare godkännande. Det är tillräckligt att tilldelas rollen som ombudsman. Undersekreteraren utnämns av Förenta staternas president, rapporterar till utrikesministern i sin roll som ombudsman, och godkänns av Förenta staternas senat i sin roll som undersekreterare. Det betonas i skrivelsen och i memorandumet att ombudsmannen är ”oberoende av Förenta staternas underrättelsegemenskap”. Arbetsgruppen ifrågasätter dock om det ministerium som ombudsmannen tillhör är det lämpligaste. Det verkar krävas en viss kännedom om och förståelse av hur underrättelsegemenskapen fungerar för att kunna fullgöra rollen som

[76] I vissa EU-medlemsstater kan enskilda personer t.ex. endast få tillgång till uppgifter som innehas av de nationella säkerhetstjänsterna genom en begäran hos högsta domstolen.

ombudsman effektivt, men samtidigt krävs det ett tillräckligt avstånd från underrättelsegemenskapen för att kunna agera oberoende.

I skölden för skydd av privatlivet anges inga särskilda kriterier för att avsätta ombudsmannen. Arbetsgruppen tolkar detta som att ombudsmannen kan avsättas från sin roll som ombudsman på samma sätt som han kan avsättas i sin roll som undersekreterare inom utrikesministeriet, vilket skulle kunna undergräva ombudsmannens ställning.

Vid första anblicken skiljer sig utnämningen av en undersekreterare i utrikesministeriet som ombudsman uppenbart från fastställandet av jurisdiktion för en vanlig domstol för en enskild persons rättsliga prövning, när det gäller oberoende. När det gäller oberoendet är frågan alltså om ombudsmannen kan anses vara likvärdig med andra oberoende tillsynsorgan som har konstaterats uppfylla kraven. När det gäller övervakning skulle detta framför allt vara Investigatory Powers Tribunal (IPT) i Storbritannien och G10-kommissionen i Tyskland.

För att avgöra detta krävs ytterligare en bedömning i form av en analys av de befogenheter som ”oberoende” myndigheter har.

*3.5.3.7 Utredningsbefogenheter*

I Kadi II-målet avgjorde EU-domstolen i fråga om artikel 47 i stadgan att ”den berörda personen måste ha möjlighet att få kännedom om de skäl som ligger till grund för det beslut som fattats rörande honom eller henne, antingen genom att läsa själva beslutet eller genom att på begäran underrättas om skälen för beslutet, vilket inte påverkar den rätt som den behöriga domstolen har att kräva att den aktuella myndigheten redovisar sina skäl (...) för att den berörde ska kunna ta till vara sina rättigheter under bästa möjliga förutsättningar”.[77] Unionsdomstolen ska förvissa sig om att det föreligger faktiska omständigheter som utgör ett tillräckligt underlag för ett sådant beslut[78]. Det anges tydligt att ”det inte kan göras gällande att uppgifterna [...] är sekretessbelagda eller hemliga”, åtminstone inte gentemot unionsdomstolen[79]. Därför drar arbetsgruppen slutsatsen att ombudsmannen måste få de uppgifter och de bevis som ligger till grund för att en åtgärd vidtas, för att uppfylla EU-domstolens krav[80].

Det är ännu oklart hur omfattande ombudsmannens utredningsbefogenheter kommer att bli. Varken kommissionens förslag till beslut eller bilaga III från utrikesministeriet är särskilt tydliga i denna fråga. Såvitt arbetsgruppen förstår skulle ombudsmannen få tillräckligt med information för att kunna fastställa om en databehandling som utförs av säkerhetstjänsterna är lagenlig och, om så inte är fallet, se till att situationen med bristande efterlevnad åtgärdas. Det anges dock inte, vare sig i skrivelsen från utrikesministeriet eller i kommissionens förslag till beslut, huruvida ombudsmannen skulle få direkt tillgång till uppgifterna om den berörda

[77] Kadi II-målet, punkt 100.
78 Kadi II-målet, punkt 119.
79 Kadi II-målet, punkt 125.
[80] Kadi II, punkt122, även om den berörda myndigheten inte måste lägga fram alla uppgifter och bevis som ligger till grund för en åtgärd.

enskilda personen och därmed skulle kunna göra en egen utredning, eller om ombudsmannen måste förlita sig enbart på rapporterna från de amerikanska myndigheternas tjänstemän.

*3.5.3.8 Befogenhet att vidta korrigerande åtgärder*

Det framgår inte särskilt tydligt av memorandumet hur ombudsmannen kan kräva att bristande efterlevnad ska åtgärdas. I kombination med bristen på tydlighet i fråga om utredningsbefogenheterna är det dessutom fortfarande oklart i vilken omfattning ombudsmannen i sig i praktiken kommer att kunna beordra åtgärder för att avhjälpa bristande efterlevnad och vad resultatet i så fall skulle bli. Kan det innebära att uppgifter som har inhämtats på ett oförenligt sätt (dvs. olagligt) inte längre får användas i något förfarande och bör raderas?

Såvitt arbetsgruppen förstår innehåller skölden för skydd av privatlivet inte heller några bestämmelser om överklagan eller granskning av ombudsmannens ”beslut”.

När det slutligen gäller ombudsmannens kommunikation med den klagande efter granskningen av ett klagomål, får ombudsmannen inte avslöja om det har förekommit något olagligt beteende hos underrättelsegemenskapen. Svaret som ges kommer alltid att vara detsamma och det kommer inte att vara specifikt. I Kadi II-målet konstaterade EU-domstolen att den behöriga myndigheten (som tillsynsmyndighet) under alla omständigheter är skyldig att ange skälen, trots att det enligt artikel 296 i EUF-fördraget inte krävs något detaljerat svar[81].

*3.5.4 Slutsats*

Arbetsgruppen tvivlar fortfarande på att det finns effektiva rättsmedel för enskilda personer. För det första ger förslaget till beslut om adekvat skyddsnivå inte något tydligt svar på frågan om i vilka situationer och under vilka förutsättningar som enskilda personer kan väcka talan för att fastställa sina rättigheter.

Arbetsgruppen erkänner och välkomnar införandet av en alternativ prövningsmekanism i form av ombudsmannen, vilket är ett unikt framsteg i förbindelserna mellan EU och ett tredjeland. Bortsett från behovet av att förtydliga begreppet *enskilda personer i EU*, som nämnts tidigare, skapar mekanismen ytterligare en möjlighet för dem att söka prövning hos de amerikanska myndigheterna för att se till att den sökandes personuppgifter behandlas i enlighet med amerikansk lagstiftning.

Samtidigt konstaterar arbetsgruppen att det framträder tydliga brister när ombudsmansmekanismen jämförs med normerna för en oberoende domstol i den mening som avses i artikel 47 i stadgan och de krav som EU-domstolen och Europadomstolen har fastställt i sin rättspraxis i övervakningsärenden. För det första finns det farhågor när det gäller huruvida ombudsmannen kan betraktas som (formellt och helt och hållet) oberoende, särskilt på grund av att det är förhållandevis lätt att avsätta politiskt utsedda personer. För det andra

[81] Kadi II-målet, punkt 116.

kvarstår farhågorna om ombudsmannens befogenhet att utöva en effektiv och kontinuerlig kontroll. Arbetsgruppen kan med utgångspunkt i den tillgängliga informationen i bilaga III inte dra slutsatsen att ombudsmannen alltid kommer att ha direkt tillgång till alla uppgifter, filer och it-system som krävs för att göra en egen bedömning eller att ombudsmannen verkligen kan tvinga de ansvariga underrättelsemyndigheterna att avbryta eventuell behandling av uppgifter som strider mot reglerna, framför allt inte om det råder oenighet om huruvida uppgiftsbehandlingen är lagenlig eller ej. Ett ytterligare förtydligande av ombudsmannens ställning och befogenheter skulle eventuellt kunna undanröja arbetsgruppens farhågor.

### 3.6 Avslutande anmärkningar om garantier och begränsningar som är tillämpliga för amerikanska nationella säkerhetsmyndigheter

För det första vill arbetsgruppen berömma kommissionen och de amerikanska myndigheterna för alla ansträngningar som har gjorts för att öka insynen i den effekt som amerikanska övervakningsprogram kan få för uppgifter som överförs inom ramen för skölden för skydd av privatlivet – eller något annat överföringsverktyg för den delen. Det har vidtagits viktiga åtgärder sedan de första avslöjandena från Edward Snowden i juni 2013, men arbetsgruppen konstaterar att det fortfarande finns farhågor. Det krävs åtminstone ytterligare förklaringar och förtydliganden av de rättigheter och skyldigheter som ingår i skölden för skydd av privatlivet.

Arbetsgruppens två viktigaste farhågor gäller det faktum att massiv och urskillningslös datainsamling inte helt och hållet utesluts av de amerikanska myndigheterna och att ombudsmannens befogenheter och ställning inte har beskrivits närmare. Dessutom bör de nationella dataskyddsmyndigheterna ha befogenhet att inleda ett förfarande hos ombudsmannen på en enskild persons vägnar, i stället för tillsynsmyndigheterna för underrättelsorganen. Arbetsgruppen är väl medveten om ansträngningarna för att avhjälpa de farhågor som dataskyddsmyndigheterna tagit upp, men ytterligare garantier skulle vara välkomna för att se till att eventuella ingrepp som orsakas av de amerikanska övervakningsprogrammen är nödvändiga i ett demokratiskt samhälle.

## 4. BEDÖMNING AV BROTTSBEKÄMPNINGSGARANTIERNA I SKÖLDEN FÖR SKYDD AV PRIVATLIVET

### 4.1 Inledning

När det gäller offentlig tillgång till personuppgifter för ändamål som rör brottsbekämpning konstaterar arbetsgruppen att de principer om skydd av privatlivet som anges i bilaga II innehåller ett undantag som är identiskt med det undantag som infördes i safe harbour-principerna. Undantagets allmänna utformning har därför bibehållits, vilket innebär att de nya principerna för skölden för skydd av privatlivet möjliggör ingrepp i de grundläggande rättigheterna för personer vars personuppgifter överförs från EU till Förenta staterna

”grundade på krav avseende nationell säkerhet, allmänintresset eller intern lagstiftning i Förenta staterna”.[82]

En av de viktigaste punkterna i den kritik som domstolen framfört mot safe harbour-beslutet i Schremsmålet var dock att det inte ”innehåller något konstaterande beträffande förekomsten i Förenta staterna av regler som antagits av staten och som syftar till att begränsa eventuella ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs från unionen till Förenta staterna”.

Därför välkomnar arbetsgruppen de amerikanska myndigheternas ansträngningar för att ge större insyn i den rättsliga ramen i fråga om ingrepp i personuppgifter som överförs inom ramen för skölden för skydd av privatlivet för ändamål som rör brottsbekämpning, däribland de tillämpliga begränsningarna och garantierna. Samtidigt understryker arbetsgruppen att detta gäller frågan om offentlig tillgång, med hänsyn till att alla inskränkningar i de grundläggande rättigheterna till privatliv och uppgiftsskydd måste gå att motivera i ett demokratiskt samhälle. Därför har arbetsgruppen analyserat brottsbekämpningsgarantierna i skölden för skydd av privatlivet utifrån den ram som beskrivs i avsnitt 1.2 i det här yttrandet.

## 4.2 Tillämpning av de europeiska grundläggande garantierna på brottsbekämpande myndigheters tillgång till uppgifter som innehas av företag

### *4.2.1 Brottsbekämpande myndigheters tillgång till personuppgifter bör vara förenlig med lagstiftningen och baseras på tydliga, exakta och lättillgängliga regler*

Bilaga VII till skölden för skydd av privatlivet innehåller en skrivelse från Förenta staternas justitieministerium med ”en kortfattad översikt av de främsta utredningsverktyg som används för att erhålla affärsuppgifter och annan information i register från företag i Förenta staterna för ändamål som rör brottsbekämpning och allmänintresset (civilt och lagstadgat), inbegripet de åtkomstbegränsningar som anges av dessa myndigheter”.

Alla förfaranden som anges i bilaga VII härrör antingen direkt från Förenta staternas konstitution (det fjärde tillägget), lagstadgade krav och processrätt eller från justitieministeriets riktlinjer och policyer. Bilaga VII innehåller dock ingen särskild hänvisning till alla de lagar där dessa förfaranden föreskrivs utan inriktas i stället på en kortfattad beskrivning av själva förfarandena. I bilaga VII anges också att det ”finns andra rättsliga grunder för företag att bestrida administrativa myndigheters förfrågningar om åtkomst till uppgifter som grundas på den bransch som företaget är verksamt i och vilka typer av uppgifter som de innehar” och det ges flera icke-uttömmande exempel, t.ex. Bank Secrecy Act, Fair Credit Reporting Act, Right to Financial Privacy Act.

Arbetsgruppen konstaterar att ramen av lagar, förfaranden och policyer är fragmenterad och att den tillämpliga rättsliga grunden för en viss begäran om tillgång beror på egenskaperna hos de uppgifter som efterfrågas, formen av företag, formen av rättsliga förfaranden

[82] Schremsmålet, punkt 87.

(straffrättsliga, administrativa, relaterade till andra allmänna intressen) och typen av enhet som begär tillgång.

Eftersom alla tillämpliga regler för att begränsa brottsbekämpande myndigheters tillgång till uppgifter som har överförts inom ramen för skölden för skydd av privatlivet baseras på konstitutionen, lagar och transparenta policyer från justitieministeriet, tar arbetsgruppen hänsyn till en presumtion om tillgänglighet i dessa regler. Huruvida dessa regler är tydliga och exakta kan emellertid bara bedömas i varje enskild typ av förfarande och begäran om tillgång. Arbetsgruppen beklagar därför att det inte går att göra en sådan bedömning för tillfället, utifrån den information som finns tillgänglig i bilaga VII till skölden för skydd av privatlivet och slutsatserna i förslaget till beslut om adekvat skyddsnivå.

### *4.2.2 Nödvändighet och proportionalitet med hänsyn till de legitima mål som eftersträvas måste påvisas*

Arbetsgruppen konstaterar att begäran om tillgång till uppgifter för ändamål som rör brottsbekämpning kan anses ha ett legitimt syfte. Enligt artikel 8.2 i Europakonventionen accepteras t.ex. att en offentlig myndighet inskränker rätten till skydd för privatlivet ”med hänsyn till (...) den allmänna säkerheten, till förebyggande av oordning eller brott”. Sådana inskränkningar är dock bara godtagbara när de är nödvändiga och proportionerliga[83].

Enligt EU-domstolens etablerade rättspraxis kräver proportionalitetsprincipen att lagförslag som inskränker rätten till privatliv och skydd för personuppgifter är ”ägnade att uppnå de legitima mål som eftersträvas med *bestämmelserna i fråga* och att de inte ska gå utöver vad som är lämpligt och nödvändigt för att uppnå dessa mål”[84] (vår kursivering). Bedömningen av nödvändighet och proportionalitet görs därför alltid i förhållande till en viss åtgärd som föreskrivs i lagstiftningen.

De amerikanska myndigheterna anger i bilaga VII att federala åklagare och federala utredare kan få tillgång till handlingar och annan registerinformation från organisationer genom ”olika typer av obligatoriska rättsprocesser, inklusive förelägganden från åtalsjuryn, administrativa förelägganden och husrannsakningsorder” och får inhämta andra meddelanden ”genom federal avlyssning i brottsbekämpande syfte samt befogenheter att utföra ’pen register’”[85]. Dessutom får myndigheter och byråer med civila och lagstadgade ansvarsområden utfärda förelägganden till organisationer om ”företagsregister, elektroniskt lagrad information eller andra materiella ting”[86]. Vidare anges i bilaga VII att dessa rättsliga förfaranden i allmänhet används för att inhämta uppgifter från ”företag” i Förenta staterna oavsett om de är certifierade inom ramen för skölden för skydd av privatlivet eller ej, och ”oavsett den

[83] Se arbetsdokumentet om europeiska grundläggande garantier, s. 7–9. En allmän bedömning av begreppen nödvändighet och proportionalitet finns i arbetsgruppens yttrande 01/2014 om tillämpningen av principerna om nödvändighet och proportionalitet samt dataskydd inom brottsbekämpningssektorn av den 27 februari 2014.
[84] Domstolens dom av den 8 april 2014, Digital Rights Ireland m.fl., förenade målen C-293/12 och C-594/12, ECLI:EU:C:2014:238, punkt 46 och rättspraxis som citeras där.
[85] Bilaga VII, s. 2.
[86] Bilaga VII, s. 4.

registrerades nationalitet". Det verkar med andra ord vara organisationerna och inte de enskilda personerna som är föremål för dessa skyddsåtgärder.

Utöver bilaga VII innehåller förslaget till beslut om adekvat skyddsnivå – som baseras på principerna för skölden för skydd av privatlivet – kommissionens slutsatser om förekomsten i Förenta staterna av regler för att begränsa inskränkningarna i de grundläggande rättigheterna för de personer vars uppgifter överförs från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet.

Slutsatserna i förslaget till beslut om adekvat skyddsnivå hänvisar framför allt till tillämpliga begränsningar och garantier enligt det fjärde tillägget till Förenta staternas konstitution, som innebär att det i princip krävs en husrannsakningsorder från domstol, grundad på "sannolika skäl", för att brottsbekämpande myndigheter ska få utföra husrannsakningar och göra beslagtaganden[87]. Slutsatserna hänvisar också till att i de undantagsfall där kravet på husrannsakningsorder inte gäller är den brottsbekämpande åtgärden föremål för ett "skälighetstest"[88].

Det framgår dock inte klart av slutsatserna hur dessa garantier tillämpas på personer som inte är amerikanska medborgare. I förslaget till beslut om adekvat skyddsnivå erkänns i själva verket i ett skäl att skyddet "enligt den fjärde ändringen inte omfattar personer från tredjeländer som inte är bosatta i Förenta staterna"[89]. Vidare anges i samma stycken i förslaget till beslut om adekvat skyddsnivå att personer från tredjeländer ändå indirekt åtnjuter detta skydd genom de amerikanska företag som innehar personuppgifterna och som tar emot förfrågningarna från de brottsbekämpande myndigheterna. Arbetsgruppen beklagar dock att denna slutsats inte hänvisar till någon rättslig källa, vare sig i lag eller i rättspraxis.

Sammantaget konstaterar arbetsgruppen att det system med utredningsverktyg som används för att erhålla affärsuppgifter och annan registrerad information i Förenta staterna för ändamål som rör brottsbekämpning och allmänintresset – inbegripet begränsningar och garantier för tillgång – är en komplex uppsättning åtgärder. Det går inte att göra någon allmän bedömning av detta system utifrån de tillgängliga uppgifterna i dag. Det krävs en särskild bedömning i individuella fall för att verkligen bedöma nödvändigheten och proportionaliteten hos de brottsbekämpande myndigheternas utredningsåtgärder i förhållande till de grundläggande rättigheterna till privatliv och uppgiftsskydd.

### *4.2.3 Det bör finnas en oberoende tillsyn*

Arbetsgruppen konstaterar att de flesta av de förfaranden som beskrivs i bilaga VII förutsätter ett domstolsbeslut innan myndigheterna kan få tillgång till uppgifterna (t.ex. domstolsbeslut om "Pen Register" och "Trap and Traces", domstolsbeslut om övervakning enligt Federal Wiretap Law, husrannsakningsorder – regel 41). Alla verkar dock inte kräva ett förhandsbeslut från en domstol. Civila och lagstadgade myndigheter får t.ex. utfärda

[87] Förslag till beslut om adekvat skyddsnivå, punkt 107.
[88] Skölden för skydd av privatlivet, punkt 107.
[89] Förslag till beslut om adekvat skyddsnivå, punkt 108.

förelägganden[90]. I dessa fall är det möjligt att göra en rättslig kontroll i efterhand av att föreläggandet var skäligt, eftersom en ”person som mottar ett administrativt föreläggande kan dessutom bestrida verkställandet av detta i domstol”[91].

Utifrån den information som finns tillgänglig konstaterar arbetsgruppen att det verkar finnas en förhållandevis kraftfull tillsynsmekanism när det gäller brottsbekämpande myndigheters tillgång till uppgifter som innehas av företag i Förenta staterna.

*4.2.4 Den enskilda personen måste ha tillgång till effektiva rättsmedel*

Skyddet enligt det fjärde tillägget omfattar som sagt inte personer från tredjeländer som inte är bosatta i Förenta staterna[92]. Detta innebär att en person från tredjeland inte skulle kunna bestrida rannsakningsorder eller framställningar i domstol med hänvisning till det fjärde tillägget. Enligt förslaget till beslut om adekvat skyddsnivå åtnjuter personer från tredjeländer ändå detta skydd indirekt, genom de amerikanska företag som innehar personuppgifterna och som tar emot förfrågningarna från de brottsbekämpande myndigheterna. Arbetsgruppen konstaterar dock att även om detta skydd skulle vara effektivt innebär det inte att enskilda personer har tillgång till effektiva rättsmedel, eftersom föremålet för rätten till ett effektivt rättsmedel i det här scenariot verkar vara det företag som tar emot begäran om tillgång och inte den enskilda person som uppgifterna rör.

Bilaga VII innehåller inte någon ytterligare information om de eventuella rättsmedel som härrör från lagar som är tillgängliga för personer från tredjeländer när myndigheter eller företag olagligen ger eller skaffar sig tillgång till innehållet i deras uppgifter.

Arbetsgruppen välkomnar att den nyligen antagna Judicial Redress Act[93] innehåller bestämmelser om rätt till rättslig prövning för personer från tredjeländer. Dessa rättigheter är emellertid begränsade till tydligt fastställda grunder för att väcka talan: rätten att få rättelse av och tillgång till uppgifter och kostnader för juridiskt bistånd när en utsedd federal myndighet eller avdelningar vägrar att ändra uppgifter eller att ge tillgång till sådana uppgifter, samt rätten till civilrättsliga åtgärder när uppgifter har lämnats ut avsiktligt och medvetet.

Den amerikanska rättspraxis som det hänvisas till i fotnoterna till de berörda skälen, särskilt City of Ontario mot Quon[94], Maryland mot King[95] och Samson mot California[96], är inte heller relevant för bedömningen av huruvida en person från tredjeland kan väcka talan vid domstol för att bestrida lagligheten i ett intrång i deras privatliv[97]. Alla mål avser rätten till

[90] Bilaga VII, s. 4.
[91] Bilaga VII, s. 4.
[92] Förslag till beslut om adekvat skyddsnivå, punkt 108.
[93] Judicial Redress Act från 2015, H.R. 1428.
[94] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson v. California*, 547 U.S. 843, 848 (2006).
[97] I Ontario mot Quon ansåg domstolen att staden Ontario inte kränkte sina anställdas rättigheter enligt fjärde tillägget eftersom stadens tillgång till den berörda anställda personens privata meddelanden var skälig, då den motiverades av ett legitimt arbetsrelaterat ändamål och inte omfattade mer än nödvändigt. I Samson mot California konstaterade domstolen att det fjärde tillägget inte förbjuder en polis att visitera en villkorligt frigiven person utan misstanke. I Maryland mot King ansåg domstolen att när poliser gör ett gripande med stöd av skälig misstanke om ett allvarligt brott och för den misstänkte

amerikanska medborgares rätt till privatliv och samtliga innehåller beslut av Förenta staternas högsta domstol som i själva verket begränsar tillämpningen av det fjärde tillägget.

Arbetsgruppen erkänner och välkomnar antagandet av Judicial Redress Act, men tvivlar fortfarande på att enskilda registrerade verkligen har tillgång till effektiva rättsmedel.

### 4.3 Avslutande kommentarer

Arbetsgruppen välkomnar och erkänner de amerikanska myndigheternas ansträngningar för att ger större insyn i den rättsliga ramen i fråga om ingrepp i personuppgifter som överförs inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna för ändamål som rör brottsbekämpning, däribland de tillämpliga begränsningarna och garantierna.

Arbetsgruppen konstaterar att systemet med de brottsbekämpande myndigheternas utredningsverktyg, däribland de tillämpliga begränsningarna och garantierna, både är omfattande och komplext och att den information som finns i skölden för skydd av privatlivet är kortfattad. Arbetsgruppen beklagar därför att den utifrån den begränsade informationen (dvs. i bilaga VII till skölden för skydd av privatlivet och i slutsatserna i förslaget till beslut om adekvat skyddsnivå) inte kan göra någon heltäckande bedömning av de tillämpliga reglernas tillgänglighet, förutsägbarhet, nödvändighet och proportionalitet vid den här tidpunkten. Oaktat arbetsgruppens övriga slutsatser om skölden för skydd av privatlivet i detta yttrande, skulle en sådan bedömning kunna ingå i en årlig översyn av skölden för skydd av privatlivet.

När det gäller de brottsbekämpande myndigheternas tillgång konstaterar arbetsgruppen att det verkar finnas en förhållandevis stark tillsynsmekanism. Dessutom välkomnar arbetsgruppen antagandet av Judicial Redress Act som innebär att även personer från tredjeland får rätt till rättslig prövning. Arbetsgruppen noterar dock att dessa rättigheter är begränsade. Utöver slutsatsen att en person från tredjeland inte skulle kunna bestrida rannsakningsorder eller förelägganden i domstol på grundval av det fjärde tillägget, kvarstår farhågorna om huruvida enskilda registrerade verkligen har tillgång till effektiva rättsmedel inom området för brottsbekämpning.

## 5. SLUTSATSER OCH REKOMMENDATIONER

För det första välkomnar arbetsgruppen att ett nytt förslag till beslut om adekvat skyddsnivå lades fram inom fem månader efter det att safe harbour-beslutet ogiltigförklarades, och att förslaget innehåller många förbättringar jämfört med den föregående mekanismen. Arbetsgruppen välkomnar framför allt den ökade insyn som erbjuds genom införandet av två förteckningar om skölden för skydd av privatlivet på handelsministeriets webbplats: en förteckning med uppgifter om de organisationer som är anslutna sill skölden för skydd av privatlivet och en förteckning med uppgifter om de organisationer som tidigare har varit anslutna, men som inte längre är det. Den ökade insynen i fråga om offentlig tillgång till

personen till polisstationen för att häktas, är provtagning av saliv och dna-analys precis som tagning av fingeravtryck och fotografering en legitim del i polisens häktningsförfarande som är skälig inom ramen för det fjärde tillägget.

uppgifter som överförts inom ramen för skölden för skydd av privatlivet för ändamål som berör nationell säkerhet eller brottsbekämpning välkomnas också. Slutligen gläder det arbetsgruppen mycket att alla överföringar av uppgifter till Förenta staterna från och med nu kommer att få samma skydd: det finns inga särskilda rättsliga bestämmelser som ger ett verktyg fördelar framför ett annat.

### 5.1 Tre frågor

Det återstår dock tre viktiga frågor som arbetsgruppen anser måste behandlas.

Den första är att ordalydelsen i förslaget till beslut om adekvat skyddsnivå inte innebär någon skyldighet för organisationerna att radera uppgifter om de inte längre är nödvändiga. Detta är en avgörande del av EU:s dataskyddslagstiftning som syftar till att säkerställa att uppgifter inte lagras längre än vad som krävs för att uppnå det ändamål för vilket uppgifterna samlades in. För det andra tolkar arbetsgruppen bilaga VI som att de amerikanska myndigheterna inte helt och hållet utesluter en fortsatt massiv och urskillningslös insamling av uppgifter. Arbetsgruppen har konsekvent framför att en sådan insamling av uppgifter är ett omotiverat ingrepp i enskilda personers grundläggande rättigheter. Den tredje frågan gäller inrättandet av en ombudsman. Arbetsgruppen välkomnar visserligen detta nya grepp för att ge enskilda personer ytterligare tillgång till prövning och tillsyn, men tvivlar fortfarande på att ombudsmannen har tillräckliga befogenheter för att kunna fungera effektivt. Ombudsmannens befogenheter och ställning bör åtminstone förtydligas, för att visa att funktionen verkligen är oberoende och kan erbjuda effektiva rättsmedel mot oförenlig uppgiftsbehandling.

### 5.2 Rekommenderade förtydliganden

Utöver de ovannämnda punkterna har arbetsgruppen lyft fram flera aspekter i detta yttrande där det bör göras ytterligare förtydliganden i beslutet om adekvat skyddsnivå. Framför allt handlar detta om behovet av att se till att viktiga dataskyddsbegrepp som används i skölden för skydd av privatlivet definieras och tillämpas på ett enhetligt sätt. Så är för närvarande inte fallet. Det vore välkommet om det infördes en ordlista över begrepp i förteckningen över vanliga frågor om skölden för skydd av privatlivet, helst med definitioner som EU och Förenta staterna har kommit överens om. Arbetsgruppen konstaterar också att regelverket för vidareöverföring av EU-personuppgifter är bristfälligt, särskilt vad avser omfattning, ändamålsbegränsning och garantier vid överföringar till förmedlare. När det gäller brottsbekämpande myndigheters tillgång till uppgifter som omfattas av skölden för skydd av privatlivet är förutsägbarheten i lagstiftningen ett orosmoment på grund av att det amerikanska brottsbekämpningssystemet är så omfattande och komplext, både på federal nivå och delstatsnivå, och att beslutet om adekvat skyddsnivå innehåller begränsad information.

Skölden för skydd av privatlivet är det första förslag till beslut om adekvat skyddsnivå som har utarbetats sedan en överenskommelse nåddes i princip om texterna till den allmänna dataskyddsförordningen. Trots detta avspeglas många av förordningens förbättringar i skyddsnivån för enskildas personuppgifter inte i skölden för skydd av privatlivet. Därför rekommenderar arbetsgruppen att det görs en översyn av detta beslut om adekvat skyddsnivå

och av de beslut om adekvat skyddsnivå som utfärdas för tredjeländer kort efter det att den allmänna dataskyddsförordningen träder i kraft.

En avslutande rekommendation från arbetsgruppen som bör lyftas fram handlar om den gemensamma översynen. Arbetsgruppen välkomnar att beslutet om adekvat skyddsnivå i skölden för skydd av privatlivet kommer att ses över årligen och att dataskyddsmyndigheter och andra relevanta parter kommer att få delta i stor omfattning. Arbetsgruppen skulle välkomna om parterna kom överens om delarna i de gemensamma översynerna och även om utformningen och presentationen av översynsrapporten i god tid före den första översynen.