EUROPEISKA
KOMMISSIONEN

Bryssel den 27.11.2013
COM(2013) 847 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU

1. INLEDNING

I direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (nedan kallat *dataskyddsdirektivet*) fastställs reglerna för överföring av personuppgifter från EU:s medlemsstater till andra länder utanför EU[1] i den mån sådana överföringar faller inom denna rättsakts tillämpningsområde[2].

Enligt direktivet kan kommissionen konstatera att ett tredjeland sörjer för en adekvat skyddsnivå på grundval av dess nationella lagstiftning eller de internationella åtaganden som landet gjort för att skydda enskildas rättigheter, i vilket fall de specifika begränsningarna för dataöverföring till det berörda landet inte är tillämpliga. Dessa beslut kallas allmänt för ***beslut om adekvat skyddsnivå***.

Den 26 juli 2000 antog kommissionen beslut 2000/520/EG[3] (nedan kallat ***safe harbour-beslutet***) där man erkänner att de principer om integritetsskydd (Safe Harbor Privacy Principles) (nedan kallade *safe harbour-principerna* eller *principerna*) och de frågor och svar (nedan kallade *frågorna och svaren* eller *FoS*) som Förenta staternas handelsministerium utfärdat, säkerställer ett adekvat skydd vid överföring av personuppgifter från EU. Safe harbour-beslutet fattades sedan en kvalificerad majoritet av medlemsstaterna avgett ett yttrande i artikel 29-gruppen respektive artikel 31-kommittén. I enlighet med rådets beslut 1999/468 granskades safe harbour-beslutet först av Europaparlamentet.

Till följd av detta möjliggör det gällande safe harbour-beslutet fri överföring[4] av personuppgifter från EU:s medlemsstater[5] till företag i Förenta staterna som har anslutit sig till principerna under omständigheter där överföringen annars inte skulle uppfylla EU:s krav på en adekvat skyddsnivå, mot bakgrund av de betydande olikheterna mellan integritetsreglerna på bägge sidor av Atlanten.

Det nuvarande safe harbour-systemet bygger på åtaganden och självcertifiering från de medverkande företagens sida. Deltagande i systemet är frivilligt, men reglerna är bindande för dem som ansluter sig. De grundläggande principerna för systemet är följande:

a) De medverkande företagens policy för integritetsskydd ska vara tillgänglig för insyn.

b) Safe harbour-principerna ska införlivas i företagens policy för integritetsskydd.

---

1 I artiklarna 25 och 26 i dataskyddsdirektivet fastställs den rättsliga ramen för överföring av personuppgifter från EU till tredjeländer utanför EES.

2 Ytterligare regler har lagts fast i artikel 13 i rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete i den mån sådana överföringar rör personuppgifter som överförs eller görs tillgängliga av en medlemsstat till en annan medlemsstat, som avser att sedan överföra dessa uppgifter till en tredjestat eller ett internationellt organ i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

3 Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, EGT L 215, 28.8.2000, s. 7.

4 Det ovanstående utesluter inte att andra krav som kan finnas i nationell lagstiftning om genomförande av EU:s dataskyddsdirektiv tillämpas på databehandlingen.

5 Dataöverföringar från de tre stater som är EES-medlemmar påverkas på ett liknande sätt till följd av utvidgningen av direktiv 95/46/EG till EES-avtalet genom beslut nr 83/1999 av den 25 juni 1999, EGT L 296, 23.11.2000, s. 41.

c) Genomförandet ska följas upp, inbegripet av offentliga myndigheter.

Dessa grundprinciper för safe harbour måste ses över mot bakgrund av de **nya omständigheterna** med

a) den exponentiella ökningen av dataflödena, som tidigare hade en stödfunktion men som numera är av central betydelse för den snabba tillväxten i den digitala ekonomin, och de mycket stora förändringarna när det gäller insamling, behandling och användning av data,

b) dataflödenas avgörande betydelse särskilt för den transatlantiska ekonomin,[6]

c) den snabba ökningen av antalet företag i Förenta Staterna som är anslutna till safe harbour-systemet; det finns nu åtta gånger fler sådana företag än 2004 (en ökning från 400 år 2004 till 3 246 år 2013),

d) de nyligen offentliggjorda uppgifterna om de amerikanska övervakningsprogrammen, som ger upphov till nya frågor om den skyddsnivå som safe harbour-systemet ska anses garantera.

Det är mot denna bakgrund som detta meddelande ger en överblick av hur safe harbour-systemet fungerar. Meddelandet **bygger på bevisning** som kommissionen samlat in, det arbete som utfördes 2009 inom EU–US Privacy Contact Group, en oberoende undersökning som utarbetades 2008[7] samt information som inhämtats inom ramen för den ad hoc-arbetsgrupp mellan EU och Förenta staterna (nedan kallad *arbetsgruppen*) som inrättats till följd av avslöjandena om Förenta staternas övervakningsprogram *(se parallellt dokument)*. Meddelandet följer på två **utvärderingsrapporter från kommissionen** som offentliggjordes under inkörningsperioden av safe harbour-systemet, 2002[8] respektive 2004[9].

2. SAFE HARBOUR-SYSTEMETS STRUKTUR OCH FUNKTIONSSÄTT

2.1. Safe harbour-systemets struktur

Ett amerikanskt företag som vill ansluta sig till safe harbour måste a) i sin allmänt tillgängliga policy för integritetsskydd ange att det ansluter sig till principerna och tillämpar dem i praktiken, och b) lämna in en självcertifiering, dvs. anmäla till Förenta Staternas handelsministerium att det efterlever principerna. Självcertifieringen ska förnyas årligen. Principerna om integritetsskydd (Safe Harbour Privacy Principles) i bilaga I till safe harbour-beslutet innefattar krav på både det materiella skyddet av personuppgifter (principer för dataintegritet, säkerhet, valmöjlighet och vidare överföring) och de registrerades processuella rättigheter (principer för meddelande, tillgång samt genomförande och uppföljning).

---

6 Om tjänster och gränsöverskridande dataflöden skulle störas till följd av att tillämpningen av bindande företagsregler, modeller för avtalsklausuler och safe harbour-systemet avbryts, skulle den negativa effekten på EU:s BNP enligt vissa undersökningar kunna uppgå till mellan -0,8 % och -1,3 % och EU:s export till Förenta staterna minska med -6,7 % på grund av försämrad konkurrenskraft. Se *The Economic Importance of Getting Data Protection Right*, en studie av European Centre for International Political Economy för den amerikanska handelskammaren (US Chamber of Commerce), mars 2013.

7 Konsekvensbedömning utarbetad 2008 för Europeiska kommissionen av *Centre de Recherche Informatique et Droit* (CRID) vid universitetet i Namur.

8 Arbetsdokument från kommissionens avdelningar om tillämpningen av kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, SEK(2002) 196, 13.12.2002.

9 Arbetsdokument från kommissionens avdelningar om genomförandet av kommissionens beslut 520/2000/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat, SEK(2004) 1323, 20.10.2004.

När det gäller genomförandet av Safe Harbour-systemet i Förenta Staterna har två amerikanska institutioner en central funktion: handelsministeriet (US Department of Commerce) och den federala konkurrensmyndigheten (US Federal Trade Commission).

Handelsministeriet kontrollerar alla safe harbour-självcertifieringar och alla årliga förnyanden av självcertifieringar som det får från företag i syfte att se till att de innehåller allt som krävs för att delta i systemet[10]. Ministeriet uppdaterar kontinuerligt en förteckning över företag som har lämnat in skrivelser om självcertifiering och offentliggör förteckningen och skrivelserna på sin webbplats. Dessutom övervakar det safe harbour-systemets funktionssätt och stryker företag som inte uppfyller kraven från förteckningen.

Den **federala konkurrensmyndigheten** ingriper, inom ramen för sina befogenheter på konsumentskyddsområdet, mot illojala eller bedrägliga metoder i enlighet med avsnitt 5 i *Free Trade Commission Act*. Till konkurrensmyndighetens verkställighetsåtgärder hör utredningar av oriktiga påståenden om att företag är anslutna till safe harbour-systemet och av bristande efterlevnad av safe harbour-principerna av företag som är medlemmar i systemet. I de specifika fall som rör uppföljning av lufttrafikföretags genomförande av safe harbour-principerna är det behöriga organet Förenta staternas transportministerium (US Department of Transportation).[11]

Det gällande safe harbour-beslutet är en del av EU:s lagstiftning som måste tillämpas av medlemsstaternas myndigheter. I beslutet föreskrivs det att EU:s nationella **dataskyddsmyndigheter** har rätt att avbryta överföringar av personuppgifter till safe harbour-certifierade företag i särskilda fall[12]. Kommissionen känner inte till några fall då överföringar skulle ha avbrutits av en nationell dataskyddsmyndighet sedan safe harbour-systemet infördes 2000. Oavsett vilka befogenheter de har enligt safe harbour-beslutet har EU:s nationella dataskyddsmyndigheter behörighet att ingripa för att säkerställa att de allmänna dataskyddsprinciperna i dataskyddsdirektivet från 1995 efterlevs, även i fråga om internationella överföringar.

Som påpekas i det gällande safe harbour-beslutet har **kommissionen befogenhet** – i enlighet med det granskningsförfarande som avses i förordning (EG) nr 182/2011 – att när som helst anpassa beslutet, upphäva det eller begränsa dess tillämpningsområde mot bakgrund av erfarenheterna av dess genomförande. Detta gäller särskilt i händelse av ett systemsammanbrott på Förenta staternas sida, t.ex. om ett organ som ansvarar för att se till att safe harbour-principerna iakttas i Förenta staterna i praktiken inte utför sina uppgifter eller om den skyddsnivå som safe harbour-principerna erbjuder är lägre än kraven i den amerikanska lagstiftningen. Liksom varje annat kommissionsbeslut kan det också ändras av andra skäl eller till och med återkallas.

---

10 Om ett företags certifiering eller förnyade certifiering inte uppfyller kraven för safe harbour meddelar handelsministeriet företaget vilka åtgärder som måste vidtas (t.ex. klargöranden, ändringar i policybeskrivningen) för att företagets certifiering ska kunna slutföras.

11 Enligt avdelning 49 i US Code Section 41712.

12 Mer specifikt kan avbrytande av överföringar krävas i två situationer, varvid
a) det amerikanska myndighetsorganet har fastställt att företaget agerar i strid med safe harbour-principerna, eller
b) det är i hög grad sannolikt att safe harbour-principerna åsidosätts, det finns välgrundad anledning att tro att den berörda tillsynsmekanismen inte vidtar eller inte i tid kommer att vidta åtgärder för att avgöra ärendet, det skulle medföra en överhängande risk för allvarlig skada för de registrerade om överföringen fortsätter, och de behöriga myndigheterna i medlemsstaterna har vidtagit efter omständigheterna rimliga åtgärder för att varna företaget och ge det möjlighet att reagera.

2.2. Safe harbour-systemets funktionssätt

Bland de **3 246**[13] **certifierade företagen** finns både små och stora företag[14]. Även om finansiella tjänster och telekommunikationssektorn ligger utanför den federala konkurrensmyndighetens tillsynsbefogenheter och därför inte omfattas av safe harbour är många andra industri- och tjänstesektorer representerade bland de certifierade företagen, inklusive välkända internetföretag och företag inom så vitt skilda områden som informations- och datatjänster, läkemedel, resetjänster och turism, hälso- och sjukvård eller kreditkortstjänster[15]. De flesta av dessa företag är amerikanska företag som tillhandahåller tjänster på EU:s inre marknad. Några av dem är dotterbolag till EU-företag som t.ex. Nokia eller Bayer. 51 % av företagen behandlar data rörande anställda i Europa som överförs till Förenta staterna i personalförvaltningssyfte[16].

Vissa dataskyddsmyndigheter i EU hyser **allt större farhågor** rörande dataöverföring inom ramen för det nuvarande safe harbour-systemet. Några medlemsstaters dataskyddsmyndigheter har kritiserat den mycket vaga formuleringen av principerna och den stora tilltron till självcertifiering och självreglering. Liknande farhågor har tagits upp av näringslivet med hänvisning till snedvridning av konkurrensen på grund av bristande tillsyn.

Det nuvarande safe harbour-systemet bygger på att företagen frivilligt ansluter sig, på de anslutna företagens självcertifiering och på att offentliga myndigheter utövar tillsyn över åtagandena inom ramen för självcertifieringen. I detta sammanhang utgör varje brist på insyn och varje brist i tillsynen ett hot mot själva grunden för safe harbour-systemet.

Eventuella luckor när det gäller insyn och tillsyn på den amerikanska sidan leder till att ansvaret vältras över till europeiska dataskyddsmyndigheter och till de företag som använder systemet. Den 29 april 2010 utfärdade den tyska dataskyddsmyndigheten ett beslut genom vilket företag som överför data från EU till Förenta staterna ålades att aktivt kontrollera att de företag i Förenta staterna som importerar data verkligen efterlever safe harbour-principerna och rekommenderades att ”åtminstone fastställa huruvida importörens safe harbour-certifiering fortfarande är giltig”[17].

Den 24 juli 2013, efter avslöjandena om Förenta staternas övervakningsprogram, gick de tyska dataskyddsmyndigheterna ett steg längre och uttryckte sin oro över ”den stora sannolikheten att principerna i kommissionens beslut överträds”[18]. Det finns fall då dataskyddsmyndigheter (t.ex. den i Bremen) har krävt att ett företag som överför personuppgifter till amerikanska leverantörer ska underrätta dataskyddsmyndigheten om huruvida och på vilket sätt de berörda leverantörerna förhindrar att den nationella säkerhetsmyndigheten (National Security Agency, NSA) får tillgång till uppgifterna. Den

---

13 Den 26 september 2013 uppgick antalet organisationer på safe harbour-förteckningen som var registrerade som ”**för närvarande anslutna**” till **3 246** och antalet ”**för närvarande ej anslutna**” till **935.**

14 Safe harbour-organisationer med högst 250 anställda: **60 %** (1 925 av 3 246). Safe harbour-organisationer med minst 251 anställda: **40 %** (1 295 av 3 246).

15 T.ex. MasterCard arbetar med tusentals banker och är ett tydligt exempel på ett fall där safe harbour-principerna inte kan ersättas med andra rättsliga instrument för överföring av personuppgifter, såsom bindande företagsregler eller avtal.

16 Safe harbour-organisationer vars certifiering omfattar organisationens personaluppgifter (och vilka därigenom har samtyckt till att samarbeta med EU:s dataskyddsmyndigheter och följa deras regler): **51 %** (1 671 av 3 246).

17 Se beslut av Düsseldorfer Kreis av den 28–29 april 2010. Se Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Europeiska datatillsynsmannen Peter Hustinx uttryckte dock vid en utfrågning i Europaparlamentets LIBE-utskott den 7 oktober 2013 uppfattningen att ”betydande förbättringar har gjorts och de flesta frågor nu är lösta” vad gäller safe harbour: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 Se resolutionen från en tysk konferens för dataskyddsombud i vilken det framhävs att underrättelsetjänster utgör ett massivt hot mot datatrafiken mellan Tyskland och länder utanför Europa: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

irländska dataskyddsmyndigheten har meddelat att den nyligen tagit emot två klagomål rörande safe harbour-programmet efter rapporteringen om den amerikanska underrättelsetjänstens program, men att den avvisat dem med motiveringen att överföringen av personuppgifter till ett tredjeland uppfyller kraven i den irländska lagstiftningen om dataskydd. Till följd av ett liknande klagomål har dataskyddsmyndigheten i Luxemburg fastslagit att Microsoft och Skype har iakttagit Luxemburgs dataskyddslagstiftning vid överföring av data till Förenta staterna[19]. Sedan dess har den irländska High Court dock bifallit en begäran om rättslig omprövning enligt vilken den kommer att granska det irländska dataskyddsombudets underlåtenhet att vidta åtgärder med avseende på USA övervakningsprogram. Ett av de två klagomålen ingavs av en grupp studerande, Europe v Facebook (EvF), som också lämnat in ett liknande klagomål mot Yahoo i Tyskland som är under behandling hos de behöriga dataskyddsmyndigheterna.

Dessa varierande reaktioner från olika dataskyddsmyndigheters sida på avslöjandena om övervakningen visar på en reell risk för fragmentisering av safe harbour-systemet och väcker frågan om i vilken utsträckning genomförandet av systemet övervakas.

3. INSYN I DE MEDVERKANDE FÖRETAGENS POLICY FÖR INTEGRITETSSKYDD

Enligt FoS 6 i bilaga II till safe harbour-beslutet måste företag som är intresserade av certifiering inom ramen för safe harbour-systemet sända sin policy för integritetsskydd till handelsministeriet och göra den tillgänglig för allmänheten. Den måste innehålla ett åtagande att följa principerna om integritetsskydd. Kravet att självcertifierade företag ska **offentliggöra sin policy för integritetsskydd** och sitt åtagande att följa principerna om integritetsskydd är av avgörande betydelse för genomförandet av systemet.

Otillräcklig tillgång till sådana företags policy för integritetsskydd är till nackdel för de enskilda vars personuppgifter samlas in och behandlas och kan innebära en **överträdelse av principen om meddelande**. I sådana fall kan enskilda personer vars uppgifter överförs från EU vara omedvetna om vilka rättigheter och skyldigheter ett självcertifierat företag har.

Vidare innebär företagens åtagande att respektera principerna om integritetsskydd att **den federala konkurrensmyndigheten har rätt att utöva tillsyn av dessa principer** med avseende på företag som underlåter att efterleva dem, t.ex. genom illojala eller bedrägliga metoder. Bristande insyn i amerikanska företag försvårar konkurrensmyndighetens övervakning och undergräver tillsynens effektivitet.

Under årens lopp har ett betydande antal självcertifierade företag underlåtit att offentliggöra sin policy för integritetsskydd och/eller att göra ett offentligt åtagande att följa principerna om integritetsskydd. Rapporten om safe harbour från 2004 pekar på behovet av att handelsministeriet **intar en mer aktiv hållning när det gäller att kontrollera** om detta krav är uppfyllt.

Sedan 2004 har handelsministeriet utvecklat **nya informationsverktyg** som syftar till att hjälpa företagen att fullgöra sina skyldigheter avseende insyn. Relevant information om systemet finns tillgänglig på handelsministeriets webbplats om safe harbour[20], där företag också kan lägga upp sin policy för integritetsskydd. Handelsministeriet har rapporterat att företag har utnyttjat denna funktion och publicerat sin policy för integritetsskydd på ministeriets webbplats i samband med att de ansökt om att ansluta sig till safe harbour[21]. Dessutom har handelsministeriet 2009–2013 offentliggjort en rad riktlinjer för företag som

[19] Se pressmeddelandet från Luxemburgs dataskyddsmyndighet av den 18 november 2013.

[20] http://www.export.gov/SafeHarbour/

[21] https://SafeHarbour.export.gov/list.aspx

vill ansluta sig till safe harbour, t.ex. *Guide to Self-Certification* och *Helpful Hints on Self-Certifying Compliance*[22].

Företagen fullgör skyldigheterna avseende insyn i varierande grad. Vissa företag inskränker sig till att meddela handelsministeriet en beskrivning av deras policy för integritetsskydd som en del av självcertifieringsprocessen, men de flesta offentliggör sin policy på sin egen webbplats vid sidan av att de laddar upp den på handelsministeriet webbplats. Det är dock **inte alltid som policyn presenteras i en användarvänlig och lättläst form**. Länkar till policyn för integritetsskydd fungerar inte alltid som de ska och leder inte heller alltid till rätt webbsidor.

Av beslutet och dess bilagor följer att kravet att företagen bör offentliggöra sin integritetsskyddspolicy **innebär mer än bara anmälan** av självcertifiering till handelsministeriet. Till de krav för certifiering som beskrivs i frågorna och svaren hör en beskrivning av policyn för integritetsskydd och tydlig information om var den finns tillgänglig för allmänheten[23]. Redogörelserna för integritetsskyddspolicyer måste vara tydliga och lätt tillgängliga för allmänheten. De måste innehålla en hyperlänk till handelsministeriet webbplats för safe harbour där förteckningar över alla ”för närvarande anslutna” medlemmar i systemet och en länk till den alternativa instansen för tvistlösning. Ett antal företag anslutna till systemet under perioden 2000–2013 har dock underlåtit att uppfylla dessa krav. I samband med arbetskontakter med kommissionen i februari 2013 medgav handelsministeriet att upp till 10 % av de certifierade företagen kan ha underlåtit att faktiskt publicera en policy för integritetsskydd som innehåller företagets åtagande att iaktta safe harbour-principerna på sin offentliga webbplats.

Färsk statistik visar också på ett ihållande problem med **oriktiga påståenden om anslutning till safe harbour**. Ca 10 % av de företag som påstår sig vara anslutna till safe harbour finns inte upptagna på handelsministeriets förteckningar över för närvarande anslutna medlemmar i systemet[24]. Sådana oriktiga påståenden kommer från både företag som aldrig har medverkat i safe harbour och företag som har anslutit sig till systemet men senare inte årligen förnyat sin självcertifiering hos handelsministeriet. I det sistnämnda fallet tas företaget fortfarande upp på förteckningen på safe harbour-webbplatsen, men med certifieringsstatus ”för närvarande ej anslutet”, vilket innebär att företaget har varit medlem i systemet och därmed är skyldigt att fortsätta att skydda data som redan behandlats. Den federala konkurrensmyndigheten är behörig att ingripa i fall av bedrägliga förfaranden och bristande efterlevnad av safe harbour-principerna (se avsnitt 5.1). Otydligheten när det gäller dessa ”oriktiga påståenden” inverkar menligt på systemets trovärdighet.

Europeiska kommissionen gjorde genom regelbundna kontakter under 2012 och 2013 handelsministeriet uppmärksamt på att det inte räcker med att företagen sänder en beskrivning av sin integritetsskyddspolicy enbart till handelsministeriet för att de ska fullgöra skyldigheterna vad gäller insyn. Redogörelserna för integritetsskyddspolicyn måste göras tillgängliga för allmänheten. Handelsministeriet ombads också att **intensifiera sina regelbundna kontroller av företagens webbplatser** efter kontrollförfarandet i samband med

---

22 Det förstnämnda dokumentet (”Guide”) finns på programmets webbplats: http://export.gov/SafeHarbour/ Dokumentet om ”Helpful Hints” finns på: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 Den 12 november 2013 bekräftade handelsministeriet att ”företag som har offentliga webbplatser och som hanterar data om konsumenter/klienter/besökare måste i nuläget ha en policy för integritetsskydd som är förenlig med safe harbour-principerna på deras respektive webbplats” (se dokumentet *U.S.-EU Cooperation to Implement the Safe Harbor Framework* av den 12 november 2013).

24 I september 2013 jämförde det australiensiska konsultföretaget Galexia ”oriktiga påståenden” om safe harbour-medlemskap under 2008 och 2013. Det viktigaste resultatet var att det parallellt med ökningen av antalet medlemmar i safe harbour-systemet mellan 2008 och 2013 (från 1 109 till 3 246) skett en ökning av antalet oriktiga påståenden från 206 till 427. http://www.galexia.com/public/about/news/about_news-id225.html

den första självcertifieringsprocessen eller den årlig förnyelsen av självcertifieringen, och att vidta åtgärder mot de företag som inte uppfyller kraven på insyn.

Som en första reaktion på farhågorna från EU:s sida har **konkurrensmyndigheten sedan mars 2013 gjort det obligatoriskt** för de företag inom safe harbour-systemet som har en offentlig webbplats att göra sin policy för integritetsskydd avseende data om kunder/användare lätt tillgänglig på denna. Samtidigt har handelsministeriet börjat meddela alla företag vars integritetsskyddspolicy inte redan innehåller en länk till handelsministeriets webbplats för safe harbour att de bör lägga till en sådan för att göra den officiella safe harbour-förteckningen och webbplatsen direkt tillgängliga för konsumenter som besöker företagets webbplats. Detta kommer att göra det möjligt för de registrerade i EU att omedelbart, utan ytterligare internetsökningar, kontrollera de åtaganden som ett företag lämnat in till handelsministeriet. Dessutom har handelsministeriet börjat meddela företagen att kontaktuppgifter för deras oberoende instans för tvistlösning bör ingå i deras publicerade integritetsskyddspolicy[25].

Denna process bör påskyndas för att säkerställa att alla certifierade företag helt och hållet uppfyller safe harbour-kraven senast i mars 2014 (då fristen för företagens årliga förnyande av certifieringen löper ut, räknat från det att de nya kraven infördes i mars 2013).

Farhågor kvarstår dock när det gäller huruvida alla självcertifierade företag helt och hållet uppfyller kraven på insyn. Uppfyllandet av de åtaganden som gjorts i samband med den ursprungliga självcertifieringen och den årliga förnyelsen av den bör övervakas och undersökas mer strikt av handelsministeriet.

4. INTEGRERING AV SAFE HARBOUR-PRINCIPERNA I FÖRETAGENS POLICYER FÖR INTEGRITETSSKYDD

Självcertifierade företag måste iaktta principerna för integritetsskydd i bilaga I till beslutet för att få ansluta sig till och fortsatt kunna åtnjuta fördelarna med safe harbour-systemet.

I rapporten från 2004 fann kommissionen att ett betydande antal **företag inte på ett korrekt sätt hade införlivat safe harbour-principerna** i sin policy för databehandling. Enskilda personer fick t.ex. inte alltid tydlig och lättbegriplig information om de ändamål för vilka uppgifterna behandlades eller gavs inte möjlighet att välja (opt out) om deras uppgifter skulle lämnas ut till en tredje part eller användas till ett ändamål som inte stämde överens med de syften för vilka de ursprungligen samlades in. I kommissionens rapport från 2004 ansågs det att handelsministeriet *borde inta en mer proaktiv hållning när det gäller tillträde till safe harbour-principerna och medvetenhet om grundprinciperna*[26].

Begränsade framsteg har gjorts i detta avseende. Sedan den 1 januari 2009 har varje företag som ansöker om att förnya sin certifieringsstatus inom safe harbour, vilket måste göras årligen, fått sin policy för integritetsskydd utvärderad av handelsministeriet innan certifieringen förnyats. Utvärderingen har emellertid begränsad räckvidd. Det finns **ingen fullständig utvärdering** av nuvarande praxis i de självcertifierade företagen som på något märkbart sätt skulle öka självcertifieringsprocessens trovärdighet.

---

25 Mellan mars och september 2013 har handelsministeriet
• meddelat de 101 företag *som redan hade laddat upp en policy för integritetsskydd som överensstämmer med safe harbour-principerna på webbsidan för safe harbour* att de också måste publicera policyn på deras företagswebbplats,
• meddelat de 154 företag som inte redan gjort det att de bör lägga till en länk till webbplatsen för safe harbour i deras integritetsskyddspolicy,
• meddelat över 600 företag att de bör lägga till kontaktuppgifter för deras oberoende instans för tvistlösning i deras integritetsskyddspolicy.

26 Se sidan 8 i rapporten; SEK(2004) 1323.

Till följd av kommissionens krav på en mer noggrann och systematisk övervakning av de självcertifierade företagen från handelsministeriets sida **ägnar man nu större uppmärksamhet åt nya ansökningar**. Antalet nya ansökningar som inte har godkänts utan har återsänts till företagen för att de ska göra förbättringar i sin policy för integritetsskydd har ökat avsevärt mellan 2010 och 2013: det har fördubblats när det gäller ansökningar om förnyad certifiering och tredubblats när det gäller nya ansökningar om anslutning till safe harbour-systemet[27]. Handelsministeriet har försäkrat kommissionen att all certifiering eller förnyande av certifiering kan slutföras endast om företagets integritetsskyddspolicy uppfyller alla krav, särskilt kravet att den ska innehålla ett åtagande om anslutning till de relevanta safe harbour-principerna och att policyn är tillgänglig för allmänheten. Ett företag är skyldigt att i sin post i safe harbour-förteckningen ange var man kan hitta den relevanta policyn. Företaget måste också på sin webbplats tydligt ange en alternativ instans för tvistlösning och lägga in en länk till safe harbour-självcertifieringen på handelsministeriets webbplats. Det uppskattas dock att över 30 % av safe harbour-medlemmarna inte lämnar någon information om tvistlösning i integritetsskyddspolicyerna på sina webbplatser[28].

En majoritet av de företag som handelsministeriet strukit från safe harbour-förteckningen ströks på de berörda företagens uttryckliga begäran (t.ex. företag som gått samman eller förvärvats, ändrat sitt verksamhetsområde eller lagt ned sin verksamhet). En mindre antal företag som upphört har strukits när de webbplatser som angetts befunnits vara ur bruk och företagens certifieringsstatus varit ”för närvarande ej anslutet” under flera år[29]. Viktigt är att ingen av dessa strykningar förefaller ha gjorts till följd av att handelsministeriets kontroll lett till att man upptäckt problem med bristande överensstämmelse.

Ett företags post i safe harbour-förteckningen fungerar som ett offentligt tillkännagivande och ett protokoll över företagets safe harbour-åtaganden. **Åtagandet att ansluta sig till safe harbour-principerna är inte tidsbegränsat** när det gäller uppgifter som mottagits under den period då företaget omfattas av safe harbour, och företaget måste fortsätta att tillämpa principerna på dessa uppgifter så länge det lagrar, använder eller lämnar ut dem, även om det av någon anledning lämnar safe-harbour-systemet.

Antalet safe harbour-**sökande som inte klarat handelsministeriets administrativa granskning** och därför aldrig förts upp på safe harbour-förteckningen är följande: År **2010** lämnades endast **6 %** (33) av de 513 företag som ansökte om certifiering för första gången utanför safe harbour-förteckningen på grund av att de inte levde upp till handelsministeriets normer för självcertifiering. År **2013** lämnades **12 %** (75) av de 605 företag som ansökte om certifiering för första gången utanför safe harbour-förteckningen på grund av att de inte levde upp till handelsministeriets normer för självcertifiering.

Som ett minimikrav för större öppenhet i tillsynen bör handelsministeriet på sin webbplats ha en förteckning över alla företag som har strukits från safe harbour-förteckningen och ange skälen till certifieringen inte har förnyats. Beteckningen ”för närvarande ej anslutet” i handelsministeriet förteckning över safe harbour-företag bör inte ses enbart som information utan åtföljas av **en tydlig varning** både i ord och grafiskt – om att ett företag för närvarande inte uppfyller kraven för safe harbour.

---

27 Enligt statistik som handelsministeriet lämnade i september 2013 uppmanade ministeriet år 2010 18 % (93) av de 512 företag som ansökte om certifiering för första gången och 16 % (231) av de 1 417 företag som förnyade sin certifiering att göra förbättringar i deras integritetsskyddspolicy och/eller ansökningar avseende safe harbour. Som en uppföljning av kommissionens krav på strikt, noggrann och systematisk kontroll av alla ansökningar uppmanade dock handelsministeriet fram till mitten av september 2013 56 % (340) av de 602 företag som ansökte om certifiering för första gången och 27 % (493) av de 1 809 företag som förnyade sin certifiering att göra förbättringar i deras integritetsskyddspolicy.

28 Enligt Chris Connolly (Galexia) vid utfrågningen i Europaparlamentets LIBE-utskott den 7 oktober 2013.

29 Fram till december 2011 hade handelsministeriet strukit 323 företag från safe harbour-förteckningen: 94 företag hade strukits för att de inte längre var verksamma, 88 till följd av förvärv eller sammanslagningar, 95 på begäran av moderbolaget, 41 till följd av upprepad underlåtenhet att ansöka om förnyad certifiering och 5 av andra skäl.

Dessutom har vissa företag ännu inte helt och hållet införlivat alla safe harbour-principerna. Vid sidan av frågan om insyn, som tas upp i avsnitt 3 ovan, är de självcertifierade företagens policyer för integritetsskydd ofta oklara när det gäller de syften för vilka uppgifter samlas in och rätten att välja huruvida uppgifter kan lämnas ut till tredje man. Detta väcker frågor om förenlighet med principerna om meddelande och valmöjlighet. Meddelande och valmöjlighet är avgörande för att garantera de registrerades kontroll över vad som händer med deras personuppgifter.

Den kritiska första steget i efterlevnadsförfarandet, att införliva safe harbour-principerna i företagens policy för integritetsskydd, säkerställs inte i tillräckligt hög grad. Handelsministeriet bör prioritera att åtgärda detta genom att utveckla en metod för efterlevnad i företagens praktiska verksamhet och deras interaktion med kunder. **Handelsministeriet måste aktivt följa upp att safe harbour-principerna faktiskt integreras i företagens integritetsskyddspolicyer,** snarare än att vidta verkställighetsåtgärder enbart till följd av klagomål från enskilda personer.

5. OFFENTLIGA MYNDIGHETERS UPPFÖLJNING AV GENOMFÖRANDET

Ett antal mekanismer finns för att garantera ett effektivt genomförande av safe harbour-systemet och ge enskilda personer möjlighet till klagomål i fall då skyddet av deras personuppgifter påverkas av bristande efterlevnad av principerna om integritetsskydd.

Enligt principen om genomförande och uppföljning måste självcertifierade organisationers policy för integritetsskydd innefatta effektiva mekanismer för att se till att principerna följs. Enligt principen om genomförande och uppföljning såsom den förtydligas i FoS 11, 5 och 6 kan detta krav uppfyllas genom användning av **oberoende rättsmedel** som offentligt har tillkännagjort sin behörighet att handlägga enskilda klagomål avseende underlåtenhet att iaktta principerna. Alternativt kan detta uppnås genom att organisationen åtar sig att samarbeta med **EU:s arbetsgrupp för dataskydd**[30]. Dessutom omfattas självcertifierade företag av den federala konkurrensmyndighetens behörighet enligt avsnitt 5 i *Federal Trade Commission Act*, som förbjuder illojala eller bedrägliga handlingar eller metoder inom handeln eller som påverkar handeln[31].

I rapporten från 2004 uttrycks farhågor när det gäller tillsynen av safe harbour-systemet och anges att den federala konkurrensmyndigheten bör inta en mer proaktiv hållning när det gäller att inleda utredningar och informera enskilda personer om deras rättigheter. Ett annat problemområde var bristen på klarhet i förhållande till konkurrensmyndighetens behörighet att övervaka efterlevnaden av principerna när det gäller personaluppgifter.

Det rättsmedel som ansvarar för personaluppgifter – EU:s arbetsgrupp för dataskydd – har tagit emot ett klagomål avseende personaluppgifter[32]. Denna avsaknad av klagomål gör det omöjligt att dra slutsatser om huruvida systemet i dess helhet fungerar väl. Kontroller på eget initiativ av företagens efterlevnad bör införas för att kontrollera det faktiska genomförandet av

30 EU:s arbetsgrupp för dataskydd är ett organ som är behörigt att undersöka och pröva klagomål från enskilda om påstådda överträdelser av safe harbour-principerna av amerikanska företag som är anslutna till safe harbour-systemet. Företag som är certifierade inom ramen för safe harbour-principerna måste välja mellan att följa ett oberoende rättsmedel eller att samarbeta med EU:s arbetsgrupp för dataskydd för att åtgärda problem som uppstår till följd av underlåtenhet att iaktta safe harbour-principerna. Samarbete med EU:s arbetsgrupp för dataskydd är dock obligatoriskt i de fall då det amerikanska företaget behandlar personaluppgifter som överförs från EU i samband med ett anställningsförhållande. Om företaget åtar sig att samarbeta med EU-arbetsgruppen måste det också åta sig att följa eventuella råd från arbetsgruppen om denna anser att företaget behöver vidta specifika åtgärder för att följa safe harbour-principerna, inklusive korrigerande eller kompenserande åtgärder.

31 Förenta staternas transportministerium utövar en liknande behörighet när det gäller lufttrafikföretag med stöd av avdelning 49 i United States Code Section 41712.

32 Klagomålet kom från en schweizisk medborgare och EU:s arbetsgrupp för dataskydd har därför hänskjutit det till den schweiziska dataskyddsmyndigheten (Förenta staterna har ett särskilt safe harbour-system för Schweiz).

åtaganden om dataskydd. EU:s dataskyddsmyndigheter bör också vidta åtgärder för att öka medvetenheten om arbetsgruppens existens.

Problem har uppmärksammats när det gäller det sätt på vilket alternativa rättsmedel fungerar som tillsynsorgan. Ett antal av dessa organ saknar lämpliga metoder för att åtgärda fall av underlåtenhet att iaktta principerna. Denna brist måste åtgärdas.

5.1. Den federala konkurrensmyndigheten (Federal Trade Commission)

Den federala konkurrensmyndigheten kan vidta verkställighetsåtgärder vid överträdelser av företagens safe harbour-åtaganden. När safe harbour-systemet inrättades åtog sig konkurrensmyndigheten att prioritera granskning av alla hänskjutningar från EU-medlemsstaternas myndigheter[33]. Eftersom inga klagomål inkommit under de första tio åren med systemet beslutade konkurrensmyndigheten att försöka identifiera eventuella överträdelser av safe harbour i varje utredning av integritetsskydd och uppgiftsskydd som den genomför. Sedan 2009 har konkurrensmyndigheten vidtagit tio verkställighetsåtgärder mot företag med anledning av safe harbour-överträdelser. Dessa åtgärder ledde i synnerhet till vitesföreläggande – belagda med betydande påföljder – med förbud mot falska uppgifter om integritetsskydd, inbegripet falska uppgifter om efterlevnad av safe harbour-principerna, och krav på heltäckande integritetsskyddsprogram och revisioner under 20 år. Företagen måste godta oberoende bedömningar av deras program för integritetsskydd på begäran av konkurrensmyndigheten. Dessa bedömningar rapporteras regelbundet till konkurrensmyndigheten. Konkurrensmyndighetens beslut förbjuder också dessa företag att ge falska uppgifter om deras praxis för integritetsskydd och deras deltagande safe harbour-systemet eller liknande system för integritetsskydd. Detta var fallet t.ex. i konkurrensmyndighetens utredningar av Google, Facebook och MySpace[34]. År 2012 godtog Google att betala böter på 22,5 miljoner US-dollar för att reda ut misstankar om att företaget hade överträtt en consent order *(*beslut om krav på samtycke). I alla utredningar som rör integritetsskydd undersöker konkurrensmyndigheten på eget initiativ om safe harbour-åtaganden har överträtts.

Den federala konkurrensmyndigheten har nyligen än en gång upprepat sina uttalanden och sitt åtagande att som en prioriterad fråga se över varje hänskjutande från företag som självreglerar sitt integritetsskydd och från EU-medlemsstater som hävdar att ett företag inte efterlever safe harbour-principerna[35]. Konkurrensmyndigheten har fått endast ett fåtal hänskjutanden från europeiska dataskyddsmyndigheter under de tre senaste åren.

Ett transatlantiskt samarbete mellan dataskyddsmyndigheter har börjat växa fram under de senaste månaderna. Till exempel undertecknade den federala konkurrensmyndigheten den 26 juni 2013 ett samförståndsavtal med Irlands dataskyddsombud om ömsesidigt bistånd vid tillsynen av lagstiftning om skydd för personuppgifter inom den privata sektorn. Genom samförståndsavtalet inrättas en ram för ett utökat, mer enhetligt och effektivare samarbete för tillsyn av integritetsskyddet[36].

---

33 Se bilaga V till rådets beslut 2000/520/EG av den 26 juli 2000.

34 Under perioden 2009–2012 slutförde konkurrensmyndigheten tio verkställighetsåtgärder avseende safe harbour-åtaganden: FTC v. Javian Karnani, och Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Se *Federal Trade Commission of Safe Harbour Commitments*: http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Se också *Case Highlights*: http://business.ftc.gov/us-eu-Safe-Harbour-framework. De flesta av dessa ärenden rör problem med företag som en gång anslutit sig till safe harbour och sedan fortsatt att utge sig som medlemmar utan att årligen förnya certifieringen.

35 Detta åtagande upprepades än en gång vid ett möte mellan chefen för den federala konkurrensmyndigheten Julie Brill och EU:s dataskyddsmyndigheter (artikel 29-gruppen) i Bryssel den 17 april 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

I augusti 2013 tillkännagav konkurrensmyndigheten att kontrollerna av företag som kontrollerar stora databaser med personuppgifter skulle skärpas ytterligare. Myndigheten har också upprättat en portal där konsumenterna kan lämna in integritetsskyddsrelaterade klagomål mot amerikanska företag[37].

Den federala konkurrensmyndigheten bör även utöka sina insatser för att undersöka oriktiga påståenden om anslutning till safe harbour. Ett företag som på sin webbplats påstår att det uppfyller kraven för safe harbour men som inte tagits upp på handelsministeriets förteckning över ”för närvarande anslutna” medlemmar vilseleder konsumenterna och missbrukar deras förtroende. Oriktiga påståenden minskar förtroendet för systemet som helhet och bör därför omedelbart tas bort från företagens webbplatser. Företagen bör vara bundna av ett verkställbart krav att konsumenterna inte får vilseledas. Konkurrensmyndigheten bör fortsätta att försöka upptäcka oriktiga påståenden om anslutning till safe harbour, som i fallet Karnani där konkurrensmyndigheten stängde en kalifornisk webbplats för att den innehöll ett oriktigt påstående om safe harbour-registrering och användes för bedrägliga metoder i samband med e-handel riktade mot europeiska konsumenter[38].

Den 29 oktober 2013 meddelade konkurrensmyndigheten att den hade inlett ”många utredningar av safe harbour-efterlevnad under de senaste månaderna” och att fler verkställighetsåtgärder på detta område kan förväntas ”under de kommande månaderna”. Konkurrensmyndigheten bekräftade också att den är ”fast besluten att undersöka hur dess effektivitet kan förbättras” och kommer att ”fortsätta att välkomna alla materiella ledtrådar, såsom det klagomål som inkommit under den senaste månaden från en EU-baserad konsumentorganisation om ett stort antal påstådda safe harbour-överträdelser”[39]. Myndigheten åtog sig också att ”systematiskt övervaka efterlevnaden av beslut inom ramen för safe harbour-systemet, på samma sätt som vi övervakar alla våra beslut[40]

Den 12 november 2013 meddelade den federala konkurrensmyndigheten Europeiska kommissionen att ”**om ett företags integritetsskyddspolicy utlovar safe harbour-skydd, kan inte det faktum att företaget inte har gjort eller bibehållit en registrering i sig innebära att företaget är undantaget från konkurrensmyndighetens tillsyn av att dessa safe harbour-åtaganden efterlevs**”[41].

I november 2013 meddelade handelsministeriet Europeiska kommissionen att ministeriet, ”för att garantera att företag inte gör oriktiga påståenden om anslutning till safe harbour-systemet, i fortsättningen kommer att kontakta safe harbour-deltagare en månad före den dag då deras certifiering ska förnyas för att beskriva vilka åtgärder de måste vidta om de väljer att avstå från att förnya den”. **Handelsministeriet ”kommer att varna företagen** i denna kategori att de måste avlägsna alla hänvisningar till safe harbour-deltagande, inbegripet användning av ministeriets safe harbour-certifieringsmärke, i företagens policyer för integritetsskydd och på deras webbplatser samt **tydligt underrätta dem om att underlåtenhet att göra detta kan göra att företagen blir föremål för verkställighetsåtgärder från den federala konkurrensmyndighetens sida**”[42].

---

37 Konsumenter kan lämna in sina klagomål via den federala konkurrensmyndighetens klagomålsassistent (Complaint Assistant) (https://www.ftccomplaintassistant.gov/) och internationella konsumenter kan lämna in klagomål via webbplatsen econsumer.gov (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf and http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Skrivelse från konkurrensmyndighetens ordförande Edith Ramirez till Europeiska kommissionens vice ordförande Viviane Reding.

41 Skrivelse från konkurrensmyndighetens ordförande Edith Ramirez till Europeiska kommissionens vice ordförande Viviane Reding.

42 *U.S.-EU Cooperation to Implement the Safe Harbor Framework* av den 12 november 2013.

För att motverka oriktiga påståenden om safe harbour-anslutning bör de självcertifierade företagens webbplatser alltid innehålla en länk till handelsministeriets safe harbour-webbsida där alla ”för närvarande anslutna” medlemmar förtecknas. På så sätt kan alla registrerade i Europa direkt, utan att behöva göra ytterligare sökningar, kontrollera om ett företag för närvarande är anslutet till safe harbour. Handelsministeriet började kräva detta av företagen i mars 2013, men processen bör påskyndas.

Den federala konkurrensmyndighetens fortlöpande övervakning och konsekventa tillsyn av att safe harbour-principerna faktiskt iakttas förblir – vid sidan av de ovannämnda åtgärder som handelsministeriet vidtar – en huvudprioritering för att se till att systemet fungerar korrekt och effektivt. Det är i synnerhet nödvändigt att öka antalet **kontroller och utredningar på eget initiativ av hur företagen efterlever** safe harbour-principerna. Det bör också bli enklare att lämna in klagomål till konkurrensmyndigheten om överträdelser.

5.2. EU:s arbetsgrupp för dataskydd

EU:s arbetsgrupp för dataskydd är ett organ som inrättats inom ramen för safe harbour-beslutet. Den har behörighet att handlägga klagomål från enskilda rörande personuppgifter som samlats in inom ramen för ett anställningsförhållande, och ärenden som gäller certifierade företag som har valt detta alternativ för tvistlösning inom safe harbour-systemet (53 % av alla företag). Arbetsgruppen består av representanter för olika dataskyddsmyndigheter i EU.

Hittills har arbetsgruppen mottagit fyra klagomål (två klagomål 2010 och två klagomål 2013). Den hänsköt år 2010 två klagomål till nationella dataskyddsmyndigheter (Förenade kungariket och Schweiz). Det tredje och det fjärde klagomålet behandlas för närvarande. Att klagomålen är så få kan förklaras av att arbetsgruppens befogenheter, som nämnts ovan, huvudsakligen begränsas till vissa typer av data.

Det begränsade antalet ärenden kan också delvis förklaras av bristande kunskap om arbetsgruppens existens. Kommissionen har sedan 2004 gjort information om arbetsgruppen mer synlig på sin webbplats[43].

För ett bättre utnyttjande av arbetsgruppen bör amerikanska företag som har valt att samarbeta med denna och följa dess beslut, när det gäller vissa eller samtliga av de kategorier av personuppgifter som omfattas av deras respektive självcertifieringar, klart och tydligt ange detta i åtagandena i sin policy för integritetsskydd så att handelsministeriet kan kontrollera denna aspekt. Alla dataskyddsmyndigheter i EU bör på sin webbplats skapa en särskild safe harbour-sida för att öka medvetenheten om safe harbour bland europeiska företag och registrerade.

5.3. Bättre genomförande och uppföljning

Den bristande insyn och de brister när det gäller genomförande och uppföljning som konstaterats ovan har gett upphov till oro bland företag i Europa när det gäller safe harbour-systemets negativa inverkan på de europeiska företagens konkurrenskraft. Om ett europeiskt företag konkurrerar med ett amerikanskt företag som deltar i safe harbour-systemet, men som

[43] I enlighet med rapporten från 2004 har ett informationsmeddelande i form av frågor och svar om EU:s arbetsgrupp för dataskydd offentliggjorts på kommissionens webbplats (GD Rättsliga frågor) för att informera enskilda och hjälpa dem att lämna in klagomål när de har anledning att tro att deras personuppgifter har behandlats i strid mot safe harbour-reglerna: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Standardblanketten för klagomål finns på http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf

i praktiken inte tillämpar dess principer, har det europeiska företaget en konkurrensnackdel i förhållande till det amerikanska företaget.

Dessutom omfattar den federala konkurrensmyndighetens behörighet illojala eller bedrägliga handlingar eller metoder i handeln och i verksamhet som påverkar handeln. I avsnitt 5 i *Federal Trade Commission Act* fastställs dock undantag till konkurrensmyndigheten befogenheter när det gäller illojala eller bedrägliga handlingar eller metoder bland annat när det gäller **telekommunikation**. Eftersom telekomföretagen inte omfattas av konkurrensmyndighetens tillsyn får de inte lov att ansluta sig till safe harbour-systemet. Med den ökande konvergensen mellan teknik och tjänster är dock många av deras direkta konkurrenter i den amerikanska IKT-sektorn medlemmar i safe harbour-systemet. Det faktum att telekomföretag är uteslutna från datautbyte inom ramen för safe harbour-systemet oroar vissa europeiska telekomoperatörer. Enligt Europeiska sammanslutningen för publika telenätoperatörer (Etno) står detta i tydlig strid med telekommunikationsoperatörernas mest angelägna krav, nämligen behovet av lika villkor[44].

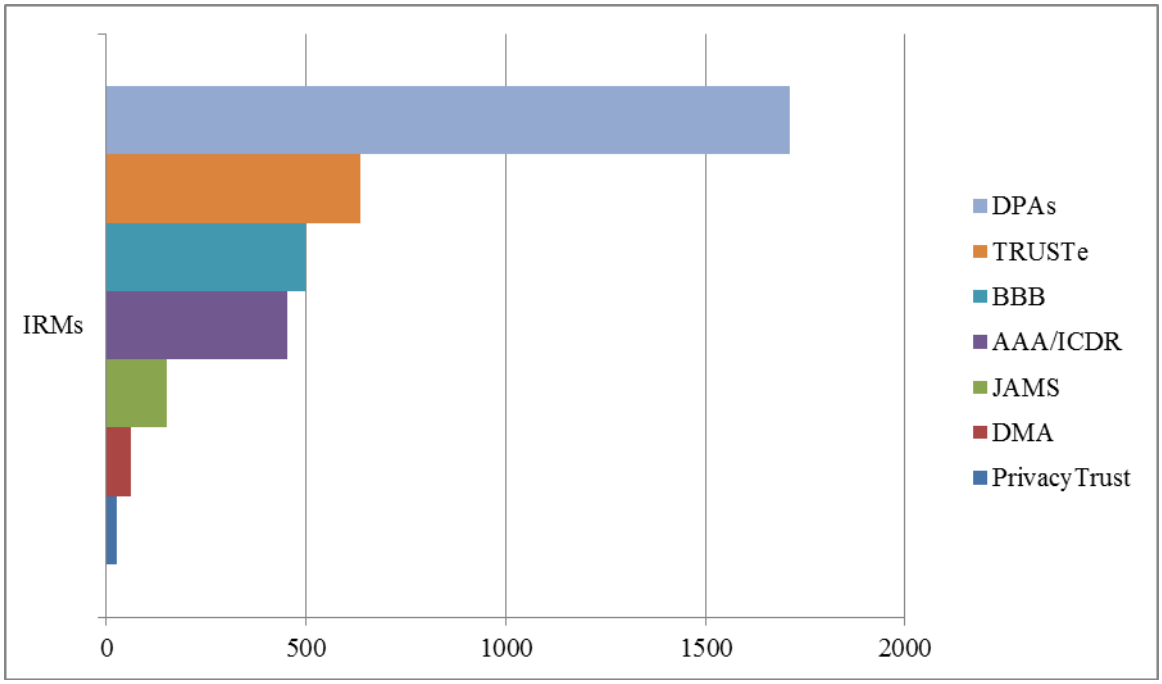
6. SKÄRPNING AV SAFE HARBOUR-PRINCIPERNA OM INTEGRITETSSKYDD

6.1. Alternativ tvistlösning

Enligt principen om genomförande och uppföljning måste det finnas ”**enkelt tillgängliga och billiga oberoende rättsmedel** genom vilka varje enskilds klagomål och tvister kan handläggas”. Inom ramen för safe harbour-systemet har det inrättats därför ett system för alternativ tvistlösning av en oberoende tredje part[45] för att tillhandahålla snabba lösningar för enskilda. De tre viktigaste organen för tvistlösning är EU:s arbetsgrupp för dataskydd, BBB (Better Business Bureaus) och TRUSTe.

44 *ETNO considerations*, som kommissionen mottog den 4 oktober 2013, tar även upp 1) definitionen av personuppgifter inom safe harbour-systemet, 2) bristen på övervakning av safe harbour, 3) det faktum att amerikanska företag kan överföra data med betydligt färre restriktioner än europeiska företag, vilket innebär en klar diskriminering av europeiska företag och påverkar de europeiska företagens konkurrenskraft. Enligt safe harbour-reglerna måste organisationer tillämpa principerna om meddelande och valmöjlighet för att få lämna uppgifter till en tredje part. Om en organisation vill överföra uppgifter till en tredje part som agerar som förmedlare kan organisationen göra detta, om den först förvissar sig om att tredje part ansluter sig till principerna eller omfattas av direktivet eller på annat sätt garanterar en adekvat skyddsnivå eller om den ingår ett skriftligt avtal med denna tredje part om att denne ska tillhandahålla minst samma integritetsskyddsnivå som krävs i principerna.

45 I EU-direktivet 2013/11/EU om alternativ tvistlösning framhålls vikten av oberoende, opartiska, öppna, effektiva, snabba och rättvisa alternativa tvistlösningsförfaranden.



Användningen av alternativ tvistlösning har ökat sedan 2004 och handelsministeriet har skärpt övervakningen av amerikanska alternativa tvistlösningsorgan för att se till att deras information om klagomålsförfarandet är tydlig, lättillgänglig och begriplig. Än så länge vet man dock inte hur effektivt detta system är, eftersom endast få ärenden hittills behandlats[46].

Även om handelsministeriet har lyckats få ner de avgifter som tas ut av de alternativa tvistlösningsorganen fortsätter två av de sju större tvistlösningsorganen att ta ut avgifter från enskilda som lämnar in klagomål[47]. Dessa anlitas av ungefär 20 % av företagen inom safe harbour-systemet. Dessa företag har valt ett tvistlösningsorgan som tar ut en avgift av konsumenter för att lämna in klagomål. Denna praxis är inte förenlig med safe harbour-principen om genomförande och uppföljning som ger enskilda rätt till tillgång till ”enkelt tillgängliga och billiga oberoende rättsmedel”. I EU är tillgången till oberoende tvistlösningstjänster som tillhandahålls av EU:s arbetsgrupp för dataskydd gratis för alla registrerade.

Den 12 november 2013 bekräftade handelsministeriet att det ”kommer att fortsätta att verka för EU-medborgarnas rätt till integritetsskydd och tillsammans med de alternativa tvistlösningsorganen undersöka om deras avgifter kan sänkas ytterligare”.

När det gäller påföljder förfogar inte alla de alternativa tvistlösningsorganen över de nödvändiga verktygen för att avhjälpa situationer där principerna för integritetsskydd inte har

[46] Exempelvis rapporterade en större tjänsteleverantör (TRUSTe) att man år 2010 mottagit 881 förfrågningar, men att endast tre av dessa ansågs godtagbara och välgrundade, vilket ledde till att de berörda företagen blev tvungna att ändra sin policy för integritetsskydd och sin webbplats. År 2011 var antalet klagomål 879, och i ett ärende blev företaget tvunget att ändra sin policy för integritetsskydd. Enligt handelsministeriet kommer större delen av klagomålen till de alternativa tvistlösningsorganen från konsumenter, till exempel användare som har glömt sitt lösenord och inte kunnat erhålla detta från sin internetleverantör. På kommissionens begäran har handelsministeriet tagit fram nya kriterier för statistikrapportering som ska användas av alla alternativa tvistlösningsorgan. Kriterierna skiljer mellan rena förfrågningar och klagomål och klargör mer utförligt de olika typer av klagomål som mottas. De nya kriterierna måste dock diskuteras ytterligare så att de nya statistikuppgifterna för 2014 omfattar alla alternativa tvistlösningsorgan, är jämförbara och ger den information som behövs för bedömningen av rättsmedlens effektivitet.

[47] International Centre for Dispute Resolution/American Arbitration Association (ICDR/AAA) tar ut 200 US-dollar och JAMS en registreringsavgift på 250 US-dollar. Handelsministeriet meddelade kommissionen att man hade arbetat med AAA, det dyraste tvistlösningsorganet för enskilda, för att utveckla ett särskilt safe harbour-program som minskade kostnaden för konsumenterna från tusentals dollar till ett fast pris på 200 US-dollar.

följts. Dessutom verkar inte alla alternativa tvistlösningsorgan tillämpa offentliggörande av konstaterade fall av bristande efterlevnad som en tillämplig påföljd eller åtgärd.

De alternativa tvistlösningsorganen måste också hänskjuta ärenden till den federala konkurrensmyndigheten om ett företag inte rättar sig efter resultatet av den alternativa tvistlösningen, eller avvisar tvistlösningsorganets beslut, så att konkurrensmyndigheten kan granska och utreda ärendet och, vid behov, vidta verkställighetsåtgärder. Hittills har dock tvistlösningsorganen inte hänskjutit några ärenden till konkurrensmyndigheten[48].

De alternativa tvistlösningsorganen har på sina webbplatser aktuella förteckningar över företag (Dispute Resolution Participants) som använder deras tjänster, vilket gör att konsumenter vid tvist med ett företag enkelt kan kontrollera om en enskild person kan lämna in ett klagomål till ett visst tvistlösningsorgan. Exempelvis förtecknar tvistlösningsorganet BBB alla företag som omfattas av BBB:s tvistlösningssystem. Det finns dock många företag som påstår att de omfattas av ett särskilt tvistlösningssystem men som inte tagits upp av de alternativa tvistlösningsorganen som deltagare i deras system[49].

Förfarandena för alternativ tvistlösning bör vara enkelt tillgängliga, oberoende och billiga för enskilda. Den registrerade bör ha möjlighet att lämna in ett klagomål utan alltför stora hinder. Alla tvistlösningsorgan bör på sina webbplatser offentliggöra statistik om de klagomål som handlagts och särskild information om resultaten av dessa. Tvistlösningsorganen bör också följas upp närmare så att deras information om förfarandet och om hur man lämnar in ett klagomål är tydlig och begriplig, och för att tvistlösning ska bli ett effektivt och tillförlitligt instrument som ger goda resultat. Det bör även upprepas att offentliggörande av konstaterade fall av bristande efterlevnad bör vara en av de obligatoriska påföljderna vid alternativ tvistlösning.

6.2. Vidare överföring

Den exponentiella tillväxten av dataflöden gör det nödvändigt att säkerställa kontinuiteten i skyddet av personuppgifter i alla skeden av databehandlingen, särskilt när data överförs av ett safe harbour-anslutet företag till en **tredje part som är registerförare**. Behovet av bättre genomförande och uppföljning av safe harbour gäller därför inte bara medlemmar i safe harbour utan även underleverantörer.

Enligt safe harbour-systemet är vidare överföring till en tredje part som agerar som ”förmedlare” tillåten om företaget – medlem i safe harbour-systemet – ”förvissar sig om att tredje part ansluter sig till principerna eller omfattas av direktivet eller på annat sätt garanterar en adekvat skyddsnivå eller om den ingår ett skriftligt avtal med denna tredje part om att denne skall tillhandahålla minst samma integritetsskyddsnivå som krävs i princip”[50]. Exempelvis kräver handelsministeriet att en leverantörer av molntjänster, som mottar personuppgifter som ska behandlas, ingår ett avtal även om denne uppfyller safe harbour-principerna[51]. Denna bestämmelse är dock inte tydlig i bilaga II till safe harbour-beslutet.

---

48 Se FoS 11.

49 Exempel: Amazon har informerat handelsministeriet om att företaget använder BBB som sitt tvistlösningsorgan. Hos BBB finns dock inte Amazon med på förteckningen över deltagare. Motsatt förhållande gäller för Arsalon Technologies (www.arsalon.net), som tillhandahåller molnvärdtjänster. Detta företag finns med på BBB:s förteckning över företag som deltar i tvistlösning inom safe harbour-systemet, men är för närvarande inte anslutet till safe harbour (den 1 oktober 2013). BBB, TRUSTe och andra alternativa tvistlösningsorgan bör ta bort eller korrigera felaktiga påståenden om certifiering. De bör vara bundna av ett verkställbart krav att endast certifiera företag som är medlemmar i safe harbour.

50 Se kommissionens beslut 2000/520/EG sidan 7 (vidare överföring).

51 Se *Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing:* http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

Eftersom användningen av underleverantörer ökat kraftigt under de senaste åren, särskilt i samband med molntjänster, bör ett företag inom safe harbour-systemet underrätta handelsministeriet när det ingår ett sådant avtal och vara skyldigt att offentliggöra de bestämmelser som rör integritetsskydd[52].

De tre ovannämnda frågorna, nämligen en alternativ tvistlösningsmekanism, förstärkt tillsyn och vidare överföring av data, bör klargöras bättre.

7. TILLGÅNG TILL UPPGIFTER SOM ÖVERFÖRS INOM RAMEN FÖR SAFE HARBOUR-SYSTEMET

Under 2013 har information om omfattningen och räckvidden av Förenta staternas övervakningsprogram gett anledning till oro för kontinuiteten i skyddet för personuppgifter som överförts lagligt till Förenta staterna inom ramen för safe harbour-systemet. Det verkar t.ex. som om alla företag som deltar i Prism-programmet och som ger de amerikanska myndigheterna tillgång till uppgifter som lagras och behandlas i Förenta staterna, är safe harbour-certifierade. Detta har gjort safe harbour-systemet till en av de kanaler genom vilken den amerikanska underrättelsetjänsten får möjlighet till att samla in personuppgifter som ursprungligen behandlats i EU.

Enligt bilaga I till safe harbour-beslutet kan efterlevnaden av principerna om integritetsskydd begränsas, om det är befogat med hänsyn till krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller till lagar, myndighetsföreskrifter eller rättspraxis. För att begränsningar och restriktioner för åtnjutande av grundläggande rättigheter ska gälla måste de tolkas restriktivt. De ska vara fastställda i allmänt tillgänglig lag och de måste vara nödvändiga och proportionerliga i ett demokratiskt samhälle. I safe harbour-beslutet specificeras särskilt att sådana begränsningar endast är tillåtna om de är begränsade till**"vad som är nödvändigt"** för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden[53]. Safe harbour-systemet medger visserligen behandling av uppgifter i undantagsfall med hänsyn till den nationella säkerheten, allmänintresset och rättsefterlevnaden, men underrättelseorganens omfattande tillgång till uppgifter som överförts till Förenta staterna i samband med handelstransaktioner var inget som kunde förutses vid antagandet av safe harbour-beslutet.

För att skapa tydlighet och rättslig säkerhet bör dessutom handelsministeriet underrätta Europeiska kommissionen om lagar eller myndighetsföreskrifter som kan inverka på anslutningen till safe harbour-principerna om integritetsskydd[54]. Användningen av undantag bör övervakas noggrant och de får inte användas på ett sätt som undergräver det skydd som

---

52 Detta gäller leverantörer av molntjänster som inte omfattas av safe harbour-systemet. Enligt konsultföretaget Galexia är andelen molntjänsteleverantörer som är medlemmar i safe harbour (och som följer principerna) relativt hög. Molntjänsteleverantörer har vanligtvis integritetsskydd i flera skikt, som ofta kombinerar direkta avtal med kunderna och den övergripande policyn för integritetsskydd. Med ett eller två viktiga undantag följer molntjänsteleverantörerna inom safe harbour de centrala bestämmelserna för tvistlösning samt för genomförande och uppföljning. I nuläget finns det inga stora molntjänstleverantörer upptagna på förteckningen över företag som använder sig av oriktiga påståenden (enligt Chris Connolly från Galexia vid utfrågningen i LIBE-utskottet om elektronisk massövervakning av EU-medborgare).

53 Se bilaga I i safe harbour-beslutet: "Efterlevnaden av principerna kan 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. I överensstämmelse med målen om ökat integritetsskydd bör organisationerna sträva efter att genomföra dessa principer öppet och fullt ut, samt även ange i sina planer för integritetsskydd på vilka områden undantag från principerna av skäl angivna i b ovan 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."

54 Yttrande 4/2000 om den dataskyddsnivå som garanteras genom safe harbor-principerna, antaget av artikel 29-gruppen den 16 maj 2000.

principerna innebär[55]. Det är framför allt de amerikanska myndigheternas omfattande tillgång till uppgifter som behandlas av självcertifierade safe harbour-företag som riskerar att undergräva konfidentialiteten vid elektronisk kommunikation.

7.1. Proportionalitet och nödvändighet

Som framgår av resultaten från ad hoc-arbetsgruppen mellan EU och Förenta staterna finns det ett antal rättsliga grunder enligt amerikansk lagstiftning som tillåter omfattande insamling och behandling av personuppgifter som lagras eller på annat sätt behandlas av företag som är baserade i Förenta staterna. Sådana uppgifter kan omfatta uppgifter som tidigare överförts från EU till Förenta staterna inom ramen för safe harbour-systemet, och det väcker frågan om safe harbour-principerna fortfarande efterlevs. Storskaligheten i dessa program kan leda till att amerikanska myndigheter får tillgång till och vidarebehandlar uppgifter som överförs inom ramen för safe harbour utöver vad som är absolut nödvändigt och proportionerligt för att skydda den nationella säkerheten enligt undantaget i safe harbour-beslutet.

7.2. Begränsningar och möjlighet till prövning

Som framgår av resultaten från ad hoc-arbetsgruppen för dataskydd mellan EU och Förenta staterna gäller garantierna enligt amerikansk lagstiftning främst amerikanska medborgare eller i Förenta staterna lagligen bosatta personer. Dessutom finns det ingen möjlighet för registrerade personer, varken i EU eller i Förenta staterna, att få tillgång till, rätta eller radera uppgifter eller möjlighet till administrativ eller rättslig prövning med avseende på insamling och vidare behandling av personuppgifter som sker inom ramen för amerikanska övervakningsprogram.

7.3. Insyn

Företagen uppger inte systematiskt i sin integritetsskyddspolicy när de tillämpar undantag från principerna. Enskilda och företag vet alltså inte vad som sker med deras uppgifter. Detta är särskilt relevant i samband med de amerikanska övervakningsprogrammen i fråga. Detta innebär att de européer vars uppgifter överförs till ett företag i Förenta staterna inom ramen för safe harbour-systemet eventuellt inte får besked från företagen om att det kan beviljas tillgång till deras uppgifter[56]. Detta väcker frågan om safe harbour-principerna för insyn efterlevs. Insyn bör garanteras så långt det är möjligt utan att den nationella säkerheten äventyras. Utöver de befintliga kraven på företagen att i sin integritetsskyddspolicy ange när principerna kan begränsas av lagar, myndighetsföreskrifter eller rättspraxis bör företag också uppmanas att i sin policy för integritetsskydd ange när de tillämpar undantag från principerna för att uppfylla krav i fråga om nationell säkerhet, allmänintresse eller rättsefterlevnad.

8. SLUTSATSER OCH REKOMMENDATIONER

Sedan safe harbour-systemet antogs 2000 har det blivit en kanal för flödena av personuppgifter mellan EU och Förenta staterna. Vikten av effektivt skydd vid överföring av personuppgifter har ökat till följd av den exponentiella ökningen av dataflöden som är av central betydelse för den digitala ekonomin, och till följd av de mycket stora förändringarna

[55] Yttrande 4/2000 om den dataskyddsnivå som garanteras genom safe harbor-principerna, antaget av artikel 29-gruppen den 16 maj 2000.

[56] Vissa europeiska företag som är med i safe harbour-systemet tillhandahåller relativt transparent information. Exempelvis anger Nokia, som bedriver verksamhet i Förenta staterna och som är medlem i safe harbour i sin policy för integritetsskydd att *”vi kan komma att pliktas enligt tvingande lag att lämna ut dina personuppgifter till vissa myndigheter eller annan tredje part, till exempel brottsbekämpande myndigheter i de länder där vi eller tredje part som handlar å våra vägnar har verksamhet.”*

när det gäller insamling, behandling och användning av data. Internetföretag som Google, Facebook, Microsoft, Apple och Yahoo har hundratals miljoner användare i Europa och överför personuppgifter för behandling i Förenta staterna i en omfattning som ingen kunde föreställa sig år 2000 då safe harbour inrättades.

På grund av bristande öppenhet och insyn och brister i genomförandet och uppföljningen av safe harbour kvarstår vissa problem som bör åtgärdas:

a) Insynen i safe-harbourmedlemmarnas policy för integritetsskydd.

b) Amerikanska företags faktiska tillämpning av principerna för integritetsskydd.

c) Effektiviteten i genomförande och uppföljning.

Underrättelseorganens **omfattande tillgång till de uppgifter som safe harbour-certifierade företag överför till Förenta staterna** ger dessutom upphov till allvarliga frågor om kontinuiteten för européers dataskyddsrättigheter när deras uppgifter överförs till Förenta staterna.

På grundval av ovanstående har kommissionen kommit fram till följande **rekommendationer**:

Öppenhet och insyn

1. *Självcertifierade företag bör offentliggöra sin policy för integritetsskydd.* Det räcker inte att företagen lämnar in en beskrivning av sin policy för integritetsskydd till handelsministeriet. Företagens policy för integritetsskydd bör göras allmänt tillgänglig på företagens webbplatser, på ett klart och tydligt språk.
2. *Självcertifierade företags webbplatser bör alltid innehålla en länk till handelsministeriets safe harbour-webbplats där alla ”för närvarande anslutna” medlemmar förtecknas.* På så sätt kan alla registrerade i Europa direkt, utan att behöva göra ytterligare sökningar, kontrollera om ett företag för närvarande är anslutet till safe harbour. Detta skulle bidra till att öka systemets trovärdighet genom att minska möjligheterna för oriktiga påståenden om att ett företag är anslutet till safe harbour. Handelsministeriet började kräva detta av företagen i mars 2013, men processen bör påskyndas.
3. *Självcertifierade företag bör offentliggöra de bestämmelser som rör integritetsskydd i alla avtal som de ingår med underleverantörer, t.ex. om datormolntjänster.* Safe harbour medger vidare överföring från självcertifierade safe harbour-företag till tredje part som agerar som förmedlare, t.ex. leverantörer av molntjänster. Så vitt känt kräver handelsministeriet i dessa fall att självcertifierade företag ska ingå ett avtal. När sådana avtal ingås bör ett safe harbour-företag dock även underrätta handelsministeriet och vara skyldigt att offentliggöra de bestämmelser som rör integritetsskydd.
4. *På handelsministeriets webbplats bör alla företag som inte för närvarande är anslutna till systemet tydligt anges.* Beteckningen ”för närvarande ej anslutet” i handelsministeriets förteckning över safe harbour-medlemmar bör åtföljas av en tydlig varning om att företaget för närvarande inte uppfyller kraven för safe harbour. Ett ”för närvarande ej anslutet” företag är dock skyldigt att fortsätta att tillämpa safe harbour-kraven för de uppgifter som det mottagit inom ramen för safe harbour.

Tvistlösning

5. *Den policy för integritetsskydd som företagen publicerar på sina webbplatser bör omfatta en länk till det alternativa tvistlösningsorganet och/eller EU:s arbetsgrupp.* Detta gör det möjligt för registrerade i Europa att omedelbart kontakta tvistlösningsorganet eller EU:s arbetsgrupp om det uppstått problem. Handelsministeriet började kräva detta av företagen i mars 2013, men processen bör påskyndas.

6. Alternativ tvistlösning bör vara lätt tillgänglig och billig. Vissa organ för alternativ tvistlösning inom ramen för safe harbour-systemet fortsätter att ta ut avgifter från enskilda – vilket kan bli mycket kostsamt för en enskild användare — för handläggning av klagomål (200–250 US-dollar). I Europa däremot kostar det inget att vända sig till den arbetsgrupp för dataskydd som inrättats för att lösa klagomål inom ramen för safe harbour.

7. *Handelsministeriet bör mer systematiskt övervaka tvistlösningsorganen i fråga om insyn i och tillgängligheten till den information som de tillhandahåller om det förfarande de tillämpar och deras uppföljning av klagomål.* Detta gör tvistlösning till ett effektivt och tillförlitligt instrument som ger goda resultat. Det bör även upprepas att offentliggörande av konstaterade fall av bristande efterlevnad bör vara en av de obligatoriska påföljderna vid alternativ tvistlösning.

Genomförande och uppföljning

8. *Efter certifiering eller förnyande av certifiering av företag inom ramen för safe harbour bör en viss andel av dessa företag bli föremål för en utredning (som omfattar mer än bara en kontroll av att de formella kraven följs) av att de i praktiken följer sin policy för integritetsskydd.*

9. *Om bristande efterlevnad konstateras till följd av ett klagomål eller en utredning bör företaget bli föremål för en särskild uppföljningsutredning efter ett år.*

10. *Vid misstanke om att ett företag brister i efterlevnaden eller vid icke avgjorda klagomål bör handelsministeriet informera den behöriga europeiska dataskyddsmyndigheten.*

11. *Oriktiga påståenden om anslutning till safe harbour bör fortsätta att utredas.* Ett företag som på sin webbplats påstår att det uppfyller kraven för safe harbour men som inte tagits upp på handelsministeriets förteckning över ”för närvarande anslutna” medlemmar vilseleder konsumenterna och missbrukar deras förtroende. Oriktiga påståenden minskar förtroendet för systemet som helhet och bör därför omedelbart tas bort från företagens webbplatser.

De amerikanska myndigheternas tillgång

12. *Självcertifierade företags policy för integritetsskydd bör innehålla uppgifter om i vilken utsträckning den amerikanska lagstiftningen tillåter offentliga myndigheter att samla in och behandla de uppgifter som överförts inom ramen för safe harbour. Framför allt bör företag uppmanas att i sin policy för integritetsskydd ange i vilka*

fall de tillämpar undantag till principerna för att uppfylla krav i fråga om nationell säkerhet, allmänintresse eller rättsefterlevnaden.

13. *Det är viktigt att undantaget avseende nationell säkerhet enligt safe harbour-beslutet endast används i en omfattning som är absolut nödvändig eller proportionerlig.*