EUROPA-
KOMMISSIONEN

Bruxelles, den 27.11.2013
COM(2013) 847 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om, hvordan safe harbor-ordningen fungerer for så vidt angår EU-borgerne og virksomhederne i EU

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om, hvordan safe harbor-ordningen fungerer for så vidt angår EU-borgerne og virksomhederne i EU

1. INDLEDNING

I direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (i det følgende benævnt "databeskyttelsesdirektivet") fastsættes reglerne for videregivelse af personoplysninger fra EU's medlemsstater til tredjelande[1], i det omfang videregivelsen falder inden for direktivets anvendelsesområde[2].

I henhold til direktivet kan Kommissionen fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau på grundlag af dets nationale lovgivning eller dets internationale forpligtelser med henblik på at beskytte personers grundlæggende rettigheder; i så fald gælder de specifikke begrænsningerne for videregivelsen af oplysninger ikke. Disse afgørelser benævnes sædvanligvis "**afgørelser om tilstrækkeligheden af beskyttelsesniveauet**".

Den 26. juli 2000 vedtog Kommissionen beslutning 520/2000/EF[3] (i det følgende benævnt "**safe harbor-beslutningen**"), hvori det anerkendes, at safe harbor-principperne til beskyttelse af privatlivets fred og de hyppige spørgsmål (i det følgende benævnt henholdsvis "principperne" og "FAQ") fra det amerikanske handelsministerium giver en tilstrækkelig beskyttelse i forbindelse med videregivelse af personoplysninger fra EU. Safe harbor-beslutningen blev truffet på grundlag af en udtalelse fra Artikel 29-Gruppen og en udtalelse fra Artikel 31-Udvalget, som blev afgivet med et kvalificeret flertal af medlemsstaterne. Safe harbor-beslutningen var genstand for en forudgående behandling i Europa-Parlamentet i henhold til Rådets afgørelse 1999/468.

Som følge heraf gør den nuværende safe harbor-beslutning det muligt frit at overføre personoplysninger[4] fra EU's medlemsstater[5] til virksomheder i USA, der har tilsluttet sig principperne, under omstændigheder, hvor overførslen ellers ikke ville opfylde EU's standarder for et tilstrækkeligt databeskyttelsesniveau på grund af de store forskelle i ordningerne til beskyttelse af privatlivets fred på de to sider af Atlanten.

Den nuværende safe harbor-ordning hviler på forpligtelser og selvcertificering fra de deltagende virksomheders side. Det er frivilligt at tilslutte sig denne ordning, men reglerne er bindende for dem, der har tilsluttet sig. De grundlæggende principper i denne ordning er:

---

1 I artikel 25 og 26 i databeskyttelsesdirektivet fastsættes de retlige rammer for videregivelse af personoplysninger fra EU til tredjelande uden for EØS.

2 Der er fastsat yderligere regler i artikel 13 i rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager, i det omfang videregivelsen vedrører personoplysninger, der af én medlemsstat videregives til eller stilles til rådighed for en anden medlemsstat, som efterfølgende har til hensigt at videregive oplysningerne til et tredjeland eller et internationalt organ med henblik på at forebygge, efterforske, afsløre eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner.

3 Kommissionens beslutning 520/2000/EF af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium, EFT L 215 af 25.8.2000, s. 7.

4 Ovenstående udelukker ikke, at andre krav, som måtte findes i den nationale lovgivning til gennemførelse af EU's databeskyttelsesdirektiv, anvendes på behandling af oplysninger.

5 Det samme gælder for videregivelse af oplysninger fra de tre stater, som er part i EØS-aftalen, efter at direktiv 95/46/EF er blevet udvidet til også at gælde EØS-aftalen, afgørelse 83/1999 af 25. juni 1999, EFT L 296 af 23.11.2000, s. 41.

a) gennemsigtighed i de deltagende virksomheders programmer til beskyttelse af privatlivets fred

b) indarbejdelse af safe harbor-principperne i virksomhedernes programmer til beskyttelse af privatlivets fred og

c) håndhævelse, bl.a. fra de offentlige myndigheders side.

Grundlaget for safe harbor-ordningen skal tages op til fornyet overvejelse i betragtning af den **nye situation**, som er karakteriseret af:

a) den eksponentielle vækst i datastrømmene, som tidligere var accessoriske, men som nu er afgørende for den digitale økonomis hurtige vækst og den meget store stigning i indsamlingen, behandlingen og anvendelsen af oplysninger

b) datastrømmenes afgørende betydning, bl.a. for den transatlantiske økonomi[6]

c) den hurtige stigning i antallet af virksomheder i USA, der har tilsluttet sig safe harbor-ordningen; der er tale om en ottedobling siden 2004 (fra 400 i 2004 til 3 246 i 2013)

d) de oplysninger, som for nylig er kommet frem om USA's overvågningsprogrammer, der rejser nye spørgsmål om det beskyttelsesniveau, som safe harbor-ordningen anses for at sikre.

På den baggrund gøres der i denne meddelelse status over, hvordan safe harbor-ordningen fungerer. Den er **baseret på dokumentation**, som er indsamlet af Kommissionen, arbejdet i EU-USA-kontaktgruppen vedrørende beskyttelse af privatlivets fred i 2009, en undersøgelse udarbejdet af en uafhængig kontrahent i 2008[7] og oplysninger, som er blevet fremlagt i EU-USA-ad hoc-arbejdsgruppen (i det følgende benævnt "arbejdsgruppen"), som blev oprettet efter afsløringerne om USA's overvågningsprogrammer (*se et parallelt dokument*). Denne meddelelse følger efter **Kommissionens to vurderingsrapporter** i safe harbor-ordningens opstartsperiode fra henholdsvis 2002[8] og 2004[9].

2. SAFE HARBOR-ORDNINGENS STRUKTUR OG FUNKTIONSMÅDE

2.1. Safe harbor-ordningens struktur

En amerikansk virksomhed, der ønsker at tilslutte sig safe harbor-ordningen, skal: a) i sit offentligt tilgængelige program til beskyttelse af privatlivets fred anføre, at den tilslutter sig principperne og rent faktisk overholder principperne, og b) foretage selvcertificering, dvs. erklære over for det amerikanske handelsministerium, at den overholder principperne. Selvcertificeringen skal fornys hvert år. Safe harbor-principperne til beskyttelse af privatlivets fred, der findes i bilag I til safe harbor-beslutningen, indeholder krav om både materiel beskyttelse af personoplysninger (principperne om dataintegritet, sikkerhed, valgfrihed og

6 Ifølge visse undersøgelser ville den negative indvirkning på EU's BNP kunne nå op på -0,8 % til -1,3 %, og EU's eksport af tjenesteydelser til USA ville falde med 6,7 % på grund af en forringelse af konkurrenceevnen, hvis tjenesterne og datastrømmene på tværs af grænserne blev afbrudt om følge af diskontinuitet i de bindende virksomhedsregler, standardaftalebestemmelserne og safe harbor-ordningen. Se: "The Economic Importance of Getting Data Protection Right", en undersøgelse foretaget af European Centre for International Political Economy for det amerikanske handelskammer, marts 2013.

7 Konsekvensanalyse udarbejdet for Europa-Kommissionen i 2008 af *Centre de Recherche Informatique et Droit* ("CRID") ved universitetet i Namur.

8 Arbejdsdokument fra Kommissionens tjenestegrene "Anvendelsen af Kommissionens beslutning 520/2000/EF af 26. juli 2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium", SEC(2002) 196 af 13.12.2002.

9 Arbejdsdokument fra Kommissionens tjenestegrene "Gennemførelsen af Kommissionens beslutning 520/2000/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium, SEC(2004) 1323 af 20.10.2004.

videre overførsel) og de registreredes processuelle rettigheder (principperne om oplysningspligt, indsigt og håndhævelse).

Med hensyn til håndhævelsen af safe harbor-ordningen i USA er der to amerikanske institutioner, som spiller en væsentlig rolle, nemlig det amerikanske handelsministerium og den amerikanske Federal Trade Commission.

Handelsministeriet kontrollerer alle safe harbor-selvcertificeringer og alle ansøgninger om årlig recertificering, som det modtager fra virksomhederne, for at sikre, at de indeholder alle de elementer, der er nødvendige for at være medlem af ordningen[10]. Det fører en liste over virksomheder, der har indsendt selvcertificeringsskrivelser, og offentliggør listen og skrivelserne på sin hjemmeside. Desuden overvåger det, hvordan safe harbor-ordningen fungerer, og fjerner virksomheder, der ikke overholder principperne, fra listen.

Federal Trade Commission griber ind mod illoyal eller vildledende praksis inden for rammerne af sine beføjelser vedrørende forbrugerbeskyttelse i henhold til paragraf 5 i Federal Trade Commission Act. Federal Trade Commissions håndhævelsesforanstaltninger omfatter bl.a. undersøgelser af urigtige erklæringer om deltagelse i safe harbor-ordningen og manglende overholdelse af disse principper i de virksomheder, der er medlemmer af ordningen. I de særlige tilfælde, hvor safe harbor-principperne skal håndhæves over for luftfartsselskaber, er det kompetente organ det amerikanske transportministerium[11].

Den nugældende safe harbor-beslutning er en del af EU-retten, som skal anvendes af myndighederne i medlemsstaterne. I henhold til beslutningen har de nationale **databeskyttelsesmyndigheder** i EU ret til at suspendere overførslen af oplysninger til safe harbor-certificerede virksomheder i bestemte tilfælde[12]. Kommissionen har ikke kendskab til tilfælde, hvor de nationale databeskyttelsesmyndigheder har suspenderet overførslen, siden safe harbor-ordningen blev indført i 2000. De nationale databeskyttelsesmyndigheder i EU har, uafhængigt af de beføjelser, de har i henhold til safe harbor-beslutningen, beføjelse til at gribe ind for at sikre, at de generelle principper om databeskyttelse i databeskyttelsesdirektivet fra 1995 overholdes, også når der er tale om internationale overførsler.

Som anført i den nugældende safe harbor-beslutning er det **Kommissionen** – som handler efter undersøgelsesproceduren i forordning 182/2011 – **der er kompetent** til til enhver tid at tilpasse beslutningen, suspendere den eller begrænse dens anvendelsesområde på grundlag af erfaringerne i forbindelse med dens gennemførelse. Det gælder specielt, hvis der er en systemisk fejl fra amerikansk side, for eksempel hvis et organ, som er ansvarligt for at sikre, at safe harbor-principperne til beskyttelse af privatlivets fred overholdes, ikke varetager sin opgave effektivt, eller hvis der i den amerikanske lovgivning stilles krav om samme beskyttelsesniveau som det, der opnås ved hjælp af safe harbor-principperne. Ligesom med Kommissionens andre beslutninger og afgørelser kan den også ændres af andre årsager eller endda tilbagekaldes.

---

10 Hvis en virksomheds certificering eller recertificering ikke opfylder safe harbor-kravene, underretter handelsministeriet virksomheden og angiver, hvilke foranstaltninger der skal træffes (f.eks. præciseringer, ændringer i beskrivelsen af programmet), inden virksomhedens certificering kan afsluttes.

11 I henhold til kapitel 49 i United States Code, paragraf 41712.

12 Mere specifikt kan overførslen af oplysninger kræves suspenderet i to tilfælde:
a) når det amerikanske regeringsorgan fastslår, at virksomheden overtræder safe harbor-principperne til beskyttelse af privatlivets fred, eller
b) når der er stor sandsynlighed for, at safe harbor-principperne til beskyttelse af privatlivets fred overtrædes, når der er rimelig grund til at antage, at det pågældende organ ikke træffer eller ikke agter at træffe passende og betimelige foranstaltninger for at løse den pågældende sag, når der ved fortsat overførsel af personoplysninger er stor risiko for på betydelig vis at skade de registrerede, og når de kompetente myndigheder i medlemsstaterne forholdene taget i betragtning på passende vis har bestræbt sig på at underrette den pågældende virksomhed og give den mulighed for at svare.

2.2. Safe harbor-ordningens funktionsmåde

De **3 246**[13] **certificerede virksomheder** omfatter både små og store virksomheder[14]. Finansielle tjenester og telesektoren ligger uden for Federal Trade Commissions håndhævelsesbeføjelser og er derfor udelukket fra safe harbor-ordningen, men der er mange industri- og tjenesteydelsessektorer, som er repræsenteret blandt de certificerede virksomheder, herunder velkendte internetvirksomheder og sektorer lige fra informations- og edb-tjenesteydelser til lægemidler, rejse- og turisttjenesteydelser, sundhedsydelser og tjenesteydelser i forbindelse med kreditkort[15]. Der er især tale om amerikanske virksomheder, som leverer tjenesteydelser i EU's indre marked. Der er også datterselskaber af en række EU-virksomheder, såsom Nokia og Bayer. 51 % er virksomheder, der behandler oplysninger om ansatte i Europa, som overføres til USA med henblik på forvaltningen af menneskelige ressourcer[16].

Hos nogle databeskyttelsesmyndigheder i EU har der været **stigende bekymring** over dataoverførsler under den nuværende safe harbor-ordning. Nogle medlemsstaters databeskyttelsesmyndigheder har kritiseret, at principperne er formuleret meget generelt, og at ordningen i høj grav hviler på selvcertificering og selvregulering. Erhvervslivet har fremsat en lignende kritik og påpeget en række forvridninger, som opstår på grund af manglende håndhævelse.

Den nuværende safe harbor-ordning hviler på, at virksomhederne frivilligt tilslutter sig principperne, på selvcertificering fra de deltagende virksomheders side og på, at de offentlige myndigheder håndhæver de forpligtelser, der følger af selvcertificeringen. I den forbindelse undergraver enhver mangel på gennemsigtighed det grundlag, som safe harbor-ordningen bygger på.

Ethvert hul i gennemsigtigheden eller håndhævelsen på den amerikanske side medfører, at ansvaret overgår til de europæiske databeskyttelsesmyndigheder og til de virksomheder, der bruger ordningen. Den 29. april 2010 udstedte de tyske databeskyttelsesmyndigheder en afgørelse, hvori de anmoder virksomheder, som overfører oplysninger fra Europa til USA, om aktivt at kontrollere, at de virksomheder i USA, som importerer oplysningerne, rent faktisk overholder safe harbor-principperne til beskyttelse af privatlivets fred, og anbefaler, at "den eksporterende virksomhed mindst skal afgøre, om importørens safe harbor-certificering stadig er gyldig"[17].

Den 24. juli 2013 gik de tyske databeskyttelsesmyndigheder efter afsløringerne om de amerikanske overvågningsprogrammer et skridt videre og udtrykte bekymring om, at "der er

---

13 Den 26. september 3013 var antallet af safe harbor-foretagender, der var opført som "**nuværende**" på safe harbor-listen, **3 246**, mens **935** var anført som "**ikke nuværende**".

14 Safe harbor-foretagender med 250 ansatte eller mindre: **60** % (1 925 ud af 3 246). Safe harbor-foretagender med 251 ansatte eller mere: **40 %** (1 295 ud af 3 246).

15 For eksempel samarbejder MasterCard med tusindvis af banker, og virksomheden er et godt eksempel på et tilfælde, hvor safe harbor-ordningen ikke kan erstattes af andre retlige instrumenter i forbindelse med overførsel af personoplysninger, såsom bindende virksomhedsregler eller kontrakter.

16 Safe harbor-foretagender, hvis safe harbor-certificering omfatter oplysninger om foretagendets menneskelige ressourcer (og som dermed har accepteret at samarbejde med EU's databeskyttelsesmyndigheder og overholde deres krav): **51 %** (1 671 ud af 3 246).

17 Se afgørelse fra Düsseldorfer Kreis af 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 Den europæiske tilsynsførende for databeskyttelse (EDPS) Peter Hustinx gav imidlertid under undersøgelsen i Europa-Parlamentets LIBE-Udvalg udtryk for, at "der er gjort betydelige fremskridt, og de fleste problemer er løst" for så vidt angår safe harbor-ordningen: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf.

stor sandsynlighed for, at principperne i Kommissionens beslutning overtrædes"[18]. Der er tilfælde, hvor en række databeskyttelsesmyndigheder (f.eks. databeskyttelsesmyndigheden i Bremen) har anmodet en virksomhed, der overfører personoplysninger til amerikanske udbydere, om at oplyse databeskyttelsesmyndigheden om, hvorvidt og hvordan de pågældende udbydere forhindrer, at National Security Agency får adgang til oplysningerne. Den irske databeskyttelsesmyndighed har rapporteret, at den for nylig har modtaget to klager med henvisning til safe harbor-programmet, efter at de amerikanske efterretningstjenesters programmer var blevet omtalt, men afviste at undersøge dem med den begrundelse, at overførslen af personoplysninger til et tredjeland opfyldte kravene i den irske databeskyttelseslovgivning. Efter en tilsvarende klage har databeskyttelsesmyndigheden i Luxembourg fastslået, at Microsoft og Skype har overholdt den luxembourgske databeskyttelseslovgivning, når de har overført oplysninger til USA[19]. Den irske højesteret har dog siden accepteret en begæring om domstolsprøvelse, hvor den vil prøve den irske databeskyttelsesmyndigheds manglende indgriben i forbindelse med de amerikanske overvågningsprogrammer. En af de to klager blev indgivet af en gruppe af studerende, Europe v Facebook (EvF), der også indgav en tilsvarende klage mod Yahoo i Tyskland, som behandles af de relevante databeskyttelsesmyndigheder.

Databeskyttelsesmyndighedernes uensartede reaktioner på afsløringerne om overvågning viser, at der er en reel risiko for fragmentering af safe harbor-ordningen, og rejser spørgsmål om, i hvilket omfang den håndhæves.

3. GENNEMSIGTIGHEDEN I DE DELTAGENDE VIRKSOMHEDERS PROGRAMMER TIL BESKYTTELSE AF PRIVATLIVETS FRED

I henhold til FAQ nr. 6, der er knyttet som bilag til safe harbor-beslutningen (bilag II), skal virksomheder, som er interesserede i certificering under safe harbor-ordningen, sende handelsministeriet en beskrivelse af virksomhedens program til beskyttelse af privatlivets fred og gøre programmet offentligt tilgængeligt. Det skal omfatte en forpligtelse til at tilslutte sig principperne til beskyttelse af privatlivets fred. Kravet om, at selvcertificerede virksomheders program til beskyttelse af privatlivets fred og deres erklæring om, at de tilslutter sig principperne til beskyttelse af privatlivets fred, skal **stilles til rådighed for offentligheden**, er afgørende for, at ordningen kan fungere.

Utilstrækkelig adgang til sådanne virksomheders programmer til beskyttelse af privatlivets fred skader de personer, hvis oplysninger indsamles og behandles, og kan udgøre en **overtrædelse af princippet om oplysningspligt**. I sådanne tilfælde er personer, hvis oplysninger overføres fra EU, ikke altid klar over deres rettigheder og de forpligtelser, som en selvcertificeret virksomhed skal overholde.

Desuden medfører virksomhedernes forpligtelse til at overholde principperne til beskyttelse af privatlivets fred, at **Federal Trade Commission har beføjelser til at håndhæve disse principper** over for virksomheder, der ikke overholder dem, idet det udgør en illoyal eller vildledende praksis. Den manglende gennemsigtighed hos de amerikanske virksomheder vanskeliggør Federal Trade Commissions kontrol og gør håndhævelsen mindre effektiv.

I årenes løb er der et betydeligt antal selvcertificerede virksomheder, som ikke har offentliggjort deres programmer til beskyttelse af privatlivets fred, og/eller som ikke har offentliggjort en erklæring om, at de tilslutter sig principperne til beskyttelse af privatlivets

[18] Se resolution fra den tyske konference for databeskyttelsesmyndigheder, hvori det fastslås, at efterretningstjenesterne udgør en stor trussel mod datatrafikken mellem Tyskland og lande uden for Europa: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

[19] Se pressemeddelelsen fra den luxembourgske databeskyttelsesmyndighed af 18. november 2013.

fred. I rapporten om safe harbor-ordningen fra 2004 fastslås det, at det amerikanske handelsministerium bør **gøre en mere aktiv indsats for at kontrollere, at dette krav overholdes**.

Siden 2004 har handelsministerriet udviklet en række **nye informationsredskaber**, der skal hjælpe virksomhederne med at overholde deres gennemsigtighedsforpligtelser. De relevante oplysninger om ordningen kan findes på handelsministeriets hjemmeside om safe harbor-ordningen[20], hvor virksomhederne også kan uploade deres programmer til beskyttelse af privatlivets fred. Handelsministeriet har rapporteret, at virksomhederne har benyttet sig af denne mulighed og offentliggjort deres program til beskyttelse af privatlivets fred på handelsministeriets hjemmeside, når de har ansøgt om tilladelse til at deltage i safe harbor-ordningen[21]. Desuden offentliggjorde handelsministeriet i 2009-2013 en række retningslinjer for virksomheder, der ønsker at deltage i safe harbor-ordningen, såsom "Guide to Self-Certification" og "Helpful Hints on Self-Certifying Compliance"[22].

Virksomhederne overholder gennemsigtighedsforpligtelserne i forskellig grad. Mens nogle virksomheder nøjes med at sende handelsministeriet en beskrivelse af deres program til beskyttelse af privatlivets fred som led i selvcertificeringsprocessen, offentliggør de fleste af virksomhederne disse programmer på deres hjemmesider, samtidig med at de uploader dem på handelsministeriets hjemmeside. Disse **programmer præsenteres dog ikke altid på en forbrugervenlig og letlæselig måde**. Hyperlinkene til programmerne til beskyttelse af privatlivets fred fungerer ikke altid ordentligt, og de fører ikke altid videre til de rigtige websteder.

Det følger af beslutningen og bilagene hertil, at kravet om, at virksomhederne skal offentliggøre deres programmer til beskyttelse af privatlivets fred, er **mere omfattende en blot at give handelsministeriet meddelelse** om selvcertificeringen. De krav til selvcertificering, som er beskrevet i FAQ, omfatter en beskrivelse af programmet til beskyttelse af privatlivets fred og gennemsigtige oplysninger om, hvor offentligheden kan få adgang til det[23]. Programmerne til beskyttelse af privatlivets fred skal være klare og let tilgængelige for offentligheden. De skal indeholde et hyperlink til handelsministeriets safe harbor-hjemmeside, som indeholder en liste over alle de "nuværende" ("current") medlemmer af ordningen og et link til instansen for alternativ tvistbilæggelse. En række af de virksomheder, der var med i ordningen i perioden 2000-2013, overholdt dog ikke disse krav. Under arbejdskontakter med Kommissionen i februar 2013 erkendte handelsministeriet, at op til 10 % af de certificerede virksomheder muligvis slet ikke har offentliggjort et program til beskyttelse af privatlivets fred, som indeholder en erklæring om overholdelse af safe harbor-ordningen, på deres respektive offentlige hjemmesider.

De seneste statistikker viser også, at der stadig er et problem med **falske påstande om tilslutning til safe harbor-ordningen**. Ca. 10 % af de virksomheder, der påstår, at de er medlem af safe harbor-ordningen, er ikke opført på handelsministeriets liste som nuværende medlemmer af ordningen[24]. De falske påstande stammer både fra virksomheder, der aldrig har

---

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

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

22 Vejledningen kan findes på programmets hjemmeside: http://export.gov/SafeHarbour/. Helpful Hints (nyttige råd): http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

23 Den 12. november 2013 bekræftede handelsministeriet, at "virksomheder, der har offentlige hjemmesider og behandler oplysninger om forbrugere/kunder/besøgende, i dag skal medtage et program til beskyttelse af privatlivets fred, der overholder safe harbor-principperne, på deres respektive hjemmesider" (dokument: "U.S.-EU Cooperation to Implement the Safe Harbor Framework" af 12. november 2013).

24 I september 2013 sammenlignede et australsk konsulentfirma, Galexia, falske påstande om medlemskab af safe harbor-ordningen i 2008 og 2013. Hovedkonklusionen er, at antallet af falske påstande er steget fra 206 til 427 mellem 2008 og 2013, parallelt med, at antallet af medlemmer af safe harbor-ordningen er steget (fra 1 109 til 3 246) http://www.galexia.com/public/about/news/about_news-id225.html.

deltaget i safe harbor-ordningen, og virksomheder, der tidligere har tilsluttet sig ordningen, men som ikke har genindsendt deres selvcertificering til handelsministeriet en gang om året. I så fald bliver de stående på safe harbor-hjemmesiden, men deres certificeringsstatus angives som "ikke nuværende" ("not current"), hvilket betyder, at virksomheden har været medlem af ordningen og dermed har pligt til fortsat at beskytte de oplysninger, som allerede er blevet behandlet. Federal Trade Commission har kompetence til at gribe ind i sager med vildledende praksis og manglende overholdelse af safe harbor-principperne (se afsnit 5.1). Uklarhed om de "falske påstande" skader ordningens troværdighed.

Europa-Kommissionen advarede gennem regelmæssige kontakter i 2012 og 2013 handelsministeriet om, at det for at overholde gennemsigtighedsforpligtelserne ikke er nok, at virksomhederne sender handelsministeriet en beskrivelse af deres program til beskyttelse af privatlivets fred. Programmerne til beskyttelse af privatlivets fred skal være tilgængelige for offentligheden. Handelsministeriet blev også bedt om at **intensivere sin periodiske kontrol af virksomhedernes hjemmesider** efter den kontrolprocedure, som gennemføres i forbindelse med den første selvcertificeringsproces eller den årlige fornyelse, og om at gribe ind over for de virksomheder, der ikke overholder gennemsigtighedskravene.

Som et første svar på EU's anmodninger **har handelsministeriet siden marts 2013 gjort det obligatorisk** for safe harbor-virksomheder med en offentlig hjemmeside at sikre, at der er let adgang til deres program til beskyttelse oplysninger om kunder/brugere på deres offentlige hjemmesider. Samtidig begyndte handelsministeriet at meddele alle virksomheder, hvis program til beskyttelse af privatlivets fred ikke allerede omfattede et link til handelsministeriets safe harbor-hjemmeside, at de skulle indsætte et sådant link, således at forbrugere, der besøger en virksomheds hjemmeside, har direkte adgang til den officielle safe harbor-liste og hjemmesiden. Det vil gøre det muligt for de registrerede i Europa med der samme at kontrollere de forpligtelser, som en virksomhed har indsendt til handelsministeriet, uden at de behøver at foretage yderligere søgninger på nettet. Desuden begyndte handelsministeriet at meddele virksomhederne, at deres offentliggjorte program til beskyttelse af privatlivets fred skal omfatte kontaktoplysninger om deres uafhængige instans for tvistbilæggelse[25].

Denne proces må fremskyndes for at sikre, at alle certificerede virksomheder fuldt ud overholder safe harbor-kravene senest i marts 2014 (hvilket er virksomhedernes årlige recertificeringsfrist, regnet fra indførelsen af de nye krav i marts 2013).

Alligevel er der stadig usikkerhed om, hvorvidt alle de selvcertificerede virksomheder fuldt ud overholder gennemsigtighedskravene. Handelsministeriet bør foretage en mere stringent overvågning og kontrol af, at virksomhederne overholder de forpligtelser, som de har påtaget sig i forbindelse med den oprindelige selvcertificering og den årlige fornyelse.

25 Mellem marts og september 2013 har handelsministeriet:
• meddelt de 101 virksomheder, *der allerede have uploadet et program til beskyttelse af privatlivets fred, der var i overensstemmelse med safe harbor-ordningen, til safe harbor-hjemmesiden*, at de også skulle offentliggøre deres program til beskyttelse af privatlivets fred på virksomhedernes hjemmesider
• meddelt de 154 virksomheder, der ikke allerede have gjort det, at de skulle medtage et link til safe harbor-hjemmesiden i deres program til beskyttelse af privatlivets fred
• meddelt over 600 virksomheder, at de skulle medtage kontaktoplysninger om deres uafhængige instans for tvistbilæggelse i deres program til beskyttelse af privatlivets fred.

4. INDARBEJDELSE AF SAFE HARBOR-PRINCIPPERNE I VIRKSOMHEDERNES PROGRAMMER TIL BESKYTTELSE AF PRIVATLIVETS FRED

Selvcertificerede virksomheder skal overholde de principper til beskyttelse af privatlivets fred, som er fastsat i bilag I til beslutningen, for at kunne opnå og beholde de fordele, som safe harbor-ordningen giver.

I rapporten fra 2004 konstaterede Kommissionen, at et stort antal **virksomheder ikke havde inkorporeret safe harbor-principperne til beskyttelse af privatlivets fred korrekt** i deres databehandlingspolitik. For eksempel fik de pågældende personer ikke altid klare og gennemsigtige oplysninger om formålene med behandlingen af deres oplysninger, eller de fik ikke mulighed for at sige nej, hvis deres oplysninger skulle videregives til tredjemand eller anvendes til et formål, som var uforeneligt med de formål, som de oprindelig blev indsamlet til. I Kommissionens rapport fra 2004 fastslås det, at handelsministeriet "*bør være mere proaktivt med hensyn til adgang til safe harbor-ordningen og kendskabet til principperne*"[26].

Der er ikke sket de store fremskridt på dette område. Siden den 1. januar 2009 har alle virksomheder, der ønsker at forny deres safe harbor-certificeringsstatus – hvilket skal ske en gang om året – fået deres program til beskyttelse af privatlivets fred vurderet af handelsministeriet inden fornyelsen. Evalueringens omfang er dog begrænset. Der foretages **ikke nogen fuldstændig evaluering af den faktiske praksis** i de selvcertificerede virksomheder; en sådan evaluering ville gøre selvcertificeringsprocessen betydeligt mere troværdig.

Som følge af Kommissionens anmodninger om et mere strengt og systematisk tilsyn med selvcertificerede selskaber fra handelsministeriets side **lægges der nu større vægt på nye ansøgninger**. Antallet af nye ansøgninger, som ikke er blevet accepteret, men er blevet sendt tilbage til virksomhederne med henblik på en forbedring af programmerne til beskyttelse af privatlivets fred, er steget betydeligt fra 2010 til 2013; der er tale om en fordobling for virksomheder, der foretager en recertificering, og en tredobling for virksomheder, der ansøger om safe harbor-certificering for første gang[27]. Handelsministeriet har forsikret Kommissionen om, at certificeringer og recertificeringer kun kan gennemføres, hvis virksomhedernes program til beskyttelse af privatlivets fred opfylde alle kravene, herunder kravet om, at det skal omfatte en positiv forpligtelse til at overholde det relevante sæt af safe harbor-principper til beskyttelse af privatlivets fred, og at programmet skal være offentligt tilgængeligt. I oplysningerne om virksomhederne på safe harbor-listen skal det angives, hvor det relevante program kan findes. Virksomhederne skal også på deres hjemmeside klart angive en instans for alternativ tvistbilæggelse og medtage et link til safe harbor-selvcertificeringen på handelsministeriets hjemmeside. Det anslås dog, at over 30 % af medlemmerne af safe harbor-ordningen ikke giver oplysninger om tvistbilæggelse i deres program til beskyttelse af privatlivets fred på deres hjemmeside[28].

Flertallet af de virksomheder, som handelsministeriet har fjernet fra safe harbor-listen, blev fjernet på udtrykkelig anmodning af de pågældende virksomheder (f.eks. virksomheder, der var fusioneret eller var blevet overtaget, havde ændret forretningsområde eller havde indstillet

---

26 Se side 8 i rapporten fra 2004, SEC(2004) 1323.

27 Ifølge statistikker, som handelsministeriet offentliggjorde i september 2013, anmodede ministeriet i 2010 18 % (93) af de 512 virksomheder, der ansøgte om certificering for første gang, og 16 % (231) af de 1 417 virksomheder, der ansøgte om recertificering, om at foretage forbedringer i deres program til beskyttelse af privatlivets fred og/eller deres safe harbor-ansøgning. Som opfølgning på Kommissionens anmodninger om en streng, omhyggelig og systematisk kontrol af alle ansøgninger anmodede handelsministeriet imidlertid frem til midten af september 2013 56 % (340) af de 602 virksomheder, der ansøgte om certificering for første gang, og 27 % (493) af de 1 809 virksomheder, der ansøgte om recertificering, om at foretage forbedringer i deres program til beskyttelse af privatlivets fred.

28 Chris Connolly (Galexia) på et møde i Europa-Parlamentets LIBE-Udvalg den 7. oktober 2013.

deres virksomhed). Et mindre antal udgåede virksomheder er blevet fjernet, når de websteder, som var angivet i oplysningerne i safe harbor-listen, ikke længere virkede, og virksomhedernes certificeringsstatus havde været "ikke nuværende" i flere år[29]. Det er værd at bemærke, at ingen af disse virksomheder er blevet fjernet, fordi handelsministeriets kontrol har medført, at der er blevet påvist problemer med overholdelsen af kravene.

Oplysningerne i safe harbor-listen fungerer som en offentlig bekendtgørelse og en registrering af virksomhedens safe harbor-forpligtelser. **Forpligtelsen til at overholde safe harbor-principperne er ikke tidsbegrænset** med hensyn til oplysninger, som modtages i den periode, hvor virksomheden nyder godt af safe harbor-ordningen, og virksomheden skal blive ved med at anvende principperne på de pågældende oplysninger, så længe den lagrer, anvender eller videregiver dem, selv hvis den af en eller anden grund forlader safe harbor-ordningen.

Antallet af **ansøgere om safe harbor-status, som ikke klarede handelsministeriets administrative kontrol** og derfor slet ikke blev optaget på safe harbor-listen, er som følger: **I 2010** var det kun **6 %** (33) af de 513 virksomheder, som ansøgte om certificering for første gang, der slet ikke blev optaget på safe harbor-listen, fordi de ikke overholdt handelsministeriets normer for selvcertificering. **I 2013** var det **12 %** (75) af de 605 virksomheder, som ansøgte om certificering for første gang, der slet ikke blev optaget på safe harbor-listen, fordi de ikke overholdt handelsministeriets normer for selvcertificering.

For at gøre kontrollen mere gennemsigtig må et mindstekrav være, at handelsministeriet på sin hjemmeside opfører alle virksomheder, der er blevet fjernet fra safe harbor-ordningen, og angiver grundene til, at certificeringen ikke er blevet fornyet. Angivelsen "ikke nuværende" på handelsministeriets liste over virksomheder, der er medlemmer af safe harbor-ordningen, bør ikke blot betragtes som en oplysning, men bør ledsages af en **klar advarsel** – både med ord og i grafisk form – om, at en virksomhed ikke på nuværende tidspunkt opfylder safe harbor-kravene.

Desuden er der stadig en række virksomheder, der ikke fuldt ud har indarbejdet safe harbor-principperne i deres program. Ud over problemet med gennemsigtighed, som er behandlet i afsnit 3 ovenfor, er der i de selvcertificerede virksomheders program til beskyttelse af privatlivets fred ofte uklarhed om formålene med indsamlingen af oplysninger og retten til at vælge, om oplysningerne må videregives til tredjemand eller ej, hvilket skaber tvivl om, hvorvidt principperne om "oplysningspligt" og "valgfrihed" er overholdt. Oplysningspligt og valgfrihed er afgørende for at sikre, at de registrerede har kontrol over, hvad der sker med deres personoplysninger.

Det første vigtige skridt i processen til sikring af, at principperne overholdes, nemlig indarbejdelsen af safe harbor-principperne til beskyttelse af privatlivets fred i programmet, garanteres ikke i tilstrækkelig grad. Handelsministeriet bør give dette spørgsmål høj prioritet ved at udvikle en metode til sikring af, at principperne overholdes i virksomhedernes operationelle praksis og i deres kontakter med kunderne. Det er vigtigt, at **handelsministeriet aktivt kontrollerer, om safe harbor-principperne effektivt er indarbejdet i virksomhedernes programmer til beskyttelse af privatlivets fred**, i stedet for, at der først træffes håndhævelsesforanstaltninger, når der indkommer klager fra fysiske personer.

[29] Ved udgangen af 2011 havde det amerikanske handelsministerium fjernet 323 virksomheder fra safe harbor-listen: 94 virksomheder blev fjernet, fordi de havde indstillet deres virksomhed, 88 virksomheder på grund af overtagelse eller fusion, 95 på anmodning af moderselskabet, 41 virksomheder på grund af, at de gentagne gange havde undladt at ansøge om recertificering og 5 virksomheder af diverse grunde.

5. HÅNDHÆVELSE FRA DE OFFENTLIGE MYNDIGHEDERS SIDE

Der findes en række mekanismer, som skal sikre, at safe harbor-ordningen håndhæves effektivt, og som skal give fysiske personer klageadgang, når beskyttelsen af deres personoplysninger ikke sikres, fordi principperne til beskyttelse af privatlivets fred ikke overholdes.

Ifølge princippet om "håndhævelse" skal selvcertificerede foretagenders programmer til beskyttelse af privatlivets fred omfatte effektive mekanismer til sikring af, at principperne overholdes. I henhold til princippet om "håndhævelse", som yderligere præciseres i FAQ nr. 11, FAQ nr. 5 og FAQ nr. 6, kan dette krav opfyldes ved tilslutning til **uafhængige klageinstanser**, som offentligt har erklæret sig kompetente til at behandle klager fra fysiske personer over manglende overholdelse af principperne. Alternativt kan dette opnås ved, at foretagendet forpligter sig til at samarbejde med **EU's Databeskyttelsespanel**[30]. Desuden er selvcertificerede virksomheder underlagt Federal Trade Commissions kompetence i henhold til Federal Trade Commission Act, der forbyder illoyal eller vildledende adfærd eller praksis i eller i forbindelse med handel[31].

I rapporten fra 2004 udtrykkes der bekymring om håndhævelsen af safe harbor-ordningen, idet det fastslås, at Federal Trade Commission bør være mere proaktiv med hensyn til at iværksætte undersøgelser og informere borgerne om deres rettigheder. Et andet område, som volder problemer, er den manglende klarhed med hensyn til Federal Trade Commissions kompetence til at håndhæve principperne i forbindelse med oplysninger om menneskelige ressourcer.

Den klageinstans, som har ansvaret for oplysninger om menneskelige ressourcer – EU's Databeskyttelsespanel – har modtaget én klage vedrørende oplysninger om menneskelige ressourcer[32]. Men selv om der ikke er indkommet klager, kan man ikke konkludere, at ordningen fungerer fuldt ud. Der bør indføres ex officio-kontrol af, om virksomhederne overholder principperne, for at undersøge, om databeskyttelsesforpligtelserne rent faktisk gennemføres. EU's databeskyttelsesmyndigheder bør også træffe foranstaltninger for at øge kendskabet til panelet.

Der er påpeget problemer med den måde, hvorpå instanserne for alternativ tvistbilæggelse fungerer som håndhævelsesorganer. En række af disse organer råder ikke over passende midler til at rette op på sager, hvor principperne ikke er blevet overholdt. Der må gøres noget ved dette problem.

5.1. Federal Trade Commission

Federal Trade Commission kan træffe håndhævelsesforanstaltninger, hvis virksomhederne ikke overholder de safe harbor-forpligtelser, de har indgået. Da safe harbor-ordningen blev indført, forpligtede Federal Trade Commission sig til at prioritere en gennemgang af alle

---

30 EU's Databeskyttelsespanel er et organ, der har kompetence til at undersøge og behandle klager fra fysiske personer om påstået overtrædeles af safe harbor-principperne begået af et amerikansk selskab, der er medlem af safe harbor-ordningen. Virksomheder, der har forpligtet sig til at overholde safe harbor-principperne, kan enten vælge at tilslutte sig en uafhængig klageinstans eller at samarbejde med EU's Databeskyttelsespanel med henblik på at afhjælpe problemer, som opstår på grund af manglende overholdelse af safe harbor-principperne. Det er dog obligatorisk at samarbejde med EU's Databeskyttelsespanel, når den amerikanske virksomhed behandler personoplysninger om menneskelige ressourcer, der overføres fra EU inden for rammerne af et ansættelsesforhold. Hvis virksomheden forpligter sig til at samarbejde med EU-panelet, skal den også forpligte sig til at rette sig efter enhver anbefaling fra EU-panelet, når det vurderer, at virksomheden skal træffe specifikke foranstaltninger for at overholde safe harbor-principperne, herunder foretage udbedrende foranstaltninger eller betale skadeserstatning.

31 Transportministeriet har en tilsvarende kompetence i forbindelse med luftfartsselskaber i henhold til kapitel 49 i United States Code, paragraf 41712.

32 Klagen kom fra en schweizisk statsborger, og EU's Databeskyttelsespanel har derfor henvist den til den schweiziske databeskyttelsesmyndighed (USA har en særskilt safe harbor-ordning for Schweiz).

sager, som henvises af myndighederne i EU's medlemsstater[33]. Da der ikke indkom nogen klager i ordningens første 10 år, besluttede Federal Trade Commission at bestræbe sig på at finde frem til eventuelle overtrædelser af safe harbor-principperne som led i alle de undersøgelser vedrørende privatlivets fred og datasikkerhed, som den foretager. Siden 2009 har Federal Trade Commission anlagt 10 håndhævelsessager mod virksomheder på grundlag af overtrædelser af safe harbor-principperne. Disse sager resulterede bl.a. i en række forligsafgørelser, som involverede store bøder, og som forbød vildledende oplysninger om bl.a. beskyttelsen af privatlivets fred, herunder om overholdelsen af safe harbor-principperne, og pålagde virksomhederne omfattende programmer til beskyttelse af privatlivets fred og revisioner i 20 år. Virksomhederne er forpligtet til at acceptere uafhængige vurderinger af deres programmer til beskyttelse af privatlivets fred på anmodning af Federal Trade Commission. Disse vurderinger indberettes regelmæssigt til Federal Trade Commission. Federal Trade Commissions afgørelser forbyder også disse virksomheder at give vildledende oplysninger om deres programmer til beskyttelse af privatlivets fred og deres deltagelse i safe harbor-ordningen eller tilsvarende private ordninger. Dette var bl.a. tilfældet i forbindelse med Federal Trade Commissions undersøgelser af Google, Facebook og Myspace[34]. I 2012 accepterede Google at betale en bøde på 22,5 mio. USD for at bilægge en tvist med påstand om, at Google overtrådte en forligsafgørelse. I forbindelse med alle undersøgelser af mulige krænkelser af privatlivets fred ser Federal Trade Commission ex officio på, om safe harbor-principperne er overtrådt.

Federal Trade Commission har for nylig gentaget sine erklæringer og løfter om, at den vil give fortrinsret til behandling af klager, der henvises af selvreguleringsvirksomheder og EU's medlemsstater, med påstand om, at en virksomhed ikke overholder safe harbor-principperne[35]. Federal Trade Commission har kun modtaget nogle få henvisninger fra de europæiske databeskyttelsesmyndigheder i de sidste tre år.

Det transatlantiske samarbejde mellem databeskyttelsesmyndighederne er begyndt at udvikle sig i de seneste måneder. For eksempel undertegnede Federal Trade Commission den 26. juni 2013 et aftalememorandum med de irske databeskyttelsesmyndigheder om gensidig bistand i håndhævelsen af lovgivningen om beskyttelse af personoplysninger i den private sektor. Med memorandummet indføres der en ramme for øget, mere strømlinet og mere effektivt samarbejde om håndhævelsen af beskyttelsen af privatlivets fred[36].

I august 2013 meddelte Federal Trade Commission, at der ville ske en yderligere skærpelse af kontrollen med virksomheder, som har kontrol over store databaser med personoplysninger. Den har også oprettet en portal, hvor forbrugerne kan indgive klage over krænkelser af privatlivets fred begået af amerikanske virksomheder[37].

Federal Trade Commission bør også øge sin indsats for at undersøge falske påstande om medlemskab af safe harbor-ordningen. En virksomhed, der på sin hjemmeside påstår, at den

---

33 Se bilag V til Kommissionens beslutning 2000/520/EF af 26. juli 2000.

34 I perioden 2009-2012 har Federal Trade Commission afsluttet 10 håndhævelsessager vedrørende safe harbor-forpligtelser: FTC mod Javian Karnani og 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 også: "Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. De fleste af disse sager drejede sig om problemer med virksomheder, som tilsluttede sig safe harbor-ordningen, men som fortsatte med at fremstille sig selv som medlemmer uden at forny den årlige certificering.

35 Løftet blev gentaget på et møde mellem Federal Trade Commission Commissioner Julie Brill og EU's databeskyttelsesmyndigheder (Artikel 29-Gruppen) i Bruxelles den 17. april 2013.

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

37 Forbrugerne kan indgive deres klager via Federal Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/), og internationale forbrugere kan indgive klager via econsumer.gov (http://www.econsumer.gov).

overholder safe harbor-kravene, men som ikke er opført på handelsministeriets liste over "nuværende" medlemmer af ordningen, vildleder forbrugerne og misbruger deres tillid. Falske påstande svækker hele systemets troværdighed og bør derfor øjeblikkelig fjernes fra virksomhedernes hjemmesider. Virksomhederne bør være pålagt et krav, der kan håndhæves, om, at de ikke må vildlede forbrugerne. Federal Trade Commission bør fortsætte med at forsøge at finde frem til falske påstande om deltagelse i safe harbor-ordningen, som det var tilfældet i *Karnani*-sagen, hvor Federal Trade Commission lukkede en californisk hjemmeside, fordi den indeholdt en falsk påstand om safe harbor-registrering og bedrev svigagtig e-handelspraksis, der var rettet mod europæiske forbrugere[38].

Den 29. oktober 2013 meddelte Federal Trade Commission, at den havde indledt "en lang række undersøgelser af overholdelsen af safe harbor-principperne i de seneste måneder", og at der kan forventes flere håndhævelsesforanstaltninger "i de kommende måneder". Federal Trade Commission bekræftede også, at den "vil bestræbe sig på at finde måder, hvorpå dens effektivitet kan forbedres" og "fortsat vil hilse alle konkrete spor velkommen, såsom den klage, den inden for den sidste måned har modtaget fra en forbrugeradvokat i Europa med påstand om en lang række overtrædelser af safe harbor-principperne"[39]. Den lovede også til "systematisk at overvåge overholdelsen af safe harbor-afgørelser, som vi gør med alle vores afgørelser"[40].

Den 12. november 2013 meddelte Federal Trade Commission Europa-Kommissionen, at "**hvis en virksomheds program til beskyttelse af privatlivets fred lover safe harbor-beskyttelse, fritager det forhold, at virksomheden ikke foretager eller opretholder en registrering, ikke i sig selv virksomheden fra håndhævelse af de pågældende safe harbor-forpligtelser fra Federal Trade Commissions side**"[41].

I november 2013 meddelte handelsministeriet Europa-Kommissionen, at det "for at bidrage til at sikre, at virksomhederne ikke fremsætter "falske påstande" om deltagelse i safe harbor-ordningen, vil begynde at kontakte safe harbor-deltagerne en måned før deres recertificeringsdato for at beskrive den procedure, de skal følge, hvis de ikke ønsker at foretage en recertificering". **Handelsministeriet "vil advare virksomhederne** i denne kategori om, at de skal fjerne alle henvisninger til deltagelse i safe harbor-ordningen, herunder brug af handelsministeriets safe harbor-certificeringsmærke, fra virksomhedernes programmer til beskyttelse af privatlivets fred og hjemmesider, **og klart meddele dem, at Federal Trade Commission vil kunne træffe håndhævelsesforanstaltninger over for virksomhederne, hvis de ikke efterkommer opfordringen**"[42].

Med henblik på at bekæmpe falske påstande om medlemskab af safe harbor-ordningen bør programmerne til beskyttelse af privatlivets fred på selvcertificerede virksomheders hjemmesider altid omfatte et link til handelsministeriets safe harbor-hjemmeside, som indeholder en liste over alle "nuværende" medlemmer af ordningen. Det vil gøre det muligt for registrerede i Europa med det samme at kontrollere, om en virksomhed på nuværende tidspunkt er medlem af safe harbor-ordningen, uden at de behøver at foretage yderligere søgninger. Handelsministeriet begyndte i marts 2013 at stille dette krav til virksomhederne, men processen bør intensiveres.

Federal Trade Commissions løbende overvågning og konsekvente håndhævelse af den faktiske overholdelse af safe harbor-principperne – i tillæg til de foranstaltninger, som

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

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

40 Brev fra formanden for Federal Trade Commission, Edith Ramirez, til næstformand Viviane Reding.

41 Brev fra formanden for Federal Trade Commission, Edith Ramirez, til næstformand Viviane Reding.

42 "U.S.-EU Cooperation to Implement the Safe Harbor Framework", 12. november 2013.

handelsministeriet har truffet, som beskrevet ovenfor – er afgørende for at sikre, at ordningen fungerer korrekt og effektivt. Det er især nødvendigt at øge **ex officio-kontrollen og undersøgelserne af virksomhedernes overholdelse** af safe harbor-principperne. Det bør også gøres endnu lettere at klage til Federal Trade Commission over overtrædelser af principperne.

5.2. EU's Databeskyttelsespanel

EU's Databeskyttelsespanel er et organ, som er oprettet i medfør af safe harbor-beslutningen. Det har kompetence til at behandle klager indgivet af fysiske personer vedrørende personoplysninger, der er indsamlet i forbindelse med arbejdsforhold, og sager vedrørende certificerede virksomheder, der har valgt denne løsning for tvistbilæggelse under safe harbor-ordningen (53 % af alle virksomhederne). Det består af repræsentanter for forskellige EU-databeskyttelsesmyndigheder.

Panelet har indtil nu modtaget fire klager (to i 2010 og to i 2013). Det henviste i 2010 to klager til nationale databeskyttelsesmyndigheder (Det Forenede Kongerige og Schweiz). Den tredje og fjerde klage er på nuværende tidspunkt under behandling. Det lave antal klager kan forklares ved, at panelets beføjelser som nævnt ovenfor hovedsagelig er begrænset til visse typer oplysninger.

Panelets begrænsede sagsmængde kan også delvis skyldes den manglende viden om, at panelet findes. Kommissionen har siden 2004 gjort oplysningerne om panelet mere synlige på sin hjemmeside[43].

For at sikre en bedre udnyttelse af panelet bør de virksomheder i USA, der for nogle af eller alle de kategorier af personoplysninger, der er omfattet af deres respektive selvcertificeringer, har valgt at samarbejde med det og overholde dets afgørelser, klart og tydeligt angive dette i deres forpligtelser vedrørende beskyttelse af privatlivets fred for at gøre det muligt for handelsministeriet at kontrollere dette aspekt. Der bør oprettes en særlig side på hver EU-databeskyttelsesmyndigheds hjemmeside vedrørende safe harbor-ordningen for at øge kendskabet til safe harbor-ordningen hos europæiske virksomheder og registrerede.

5.3. Bedre håndhævelse

De svagheder i gennemsigtigheden og håndhævelsen, som påpeges ovenfor, giver anledning til bekymring blandt europæiske virksomheder over safe harbor-ordningens negative indvirkning på europæiske virksomheders konkurrenceevne. Når en europæisk virksomhed konkurrerer med en amerikansk virksomhed, der er medlem af safe harbor-ordningen, men som i praksis ikke anvender safe harbor-principperne, stilles den europæiske virksomhed konkurrencemæssigt ringere end den amerikanske virksomhed.

Desuden omfatter Federal Trade Commissions kompetence kun illoyal eller vildledende adfærd eller praksis, "hvis de er handelsrelaterede". I henhold til paragraf 5 i Federal Trade Commission Act er der dog en række områder, hvor Federal Trade Commission ikke har kompetence vedrørende illoyal eller vildledende adfærd eller praksis, bl.a. **telekommunikation**. Da telekommunikationsselskaber ikke er omfattet af Federal Trade

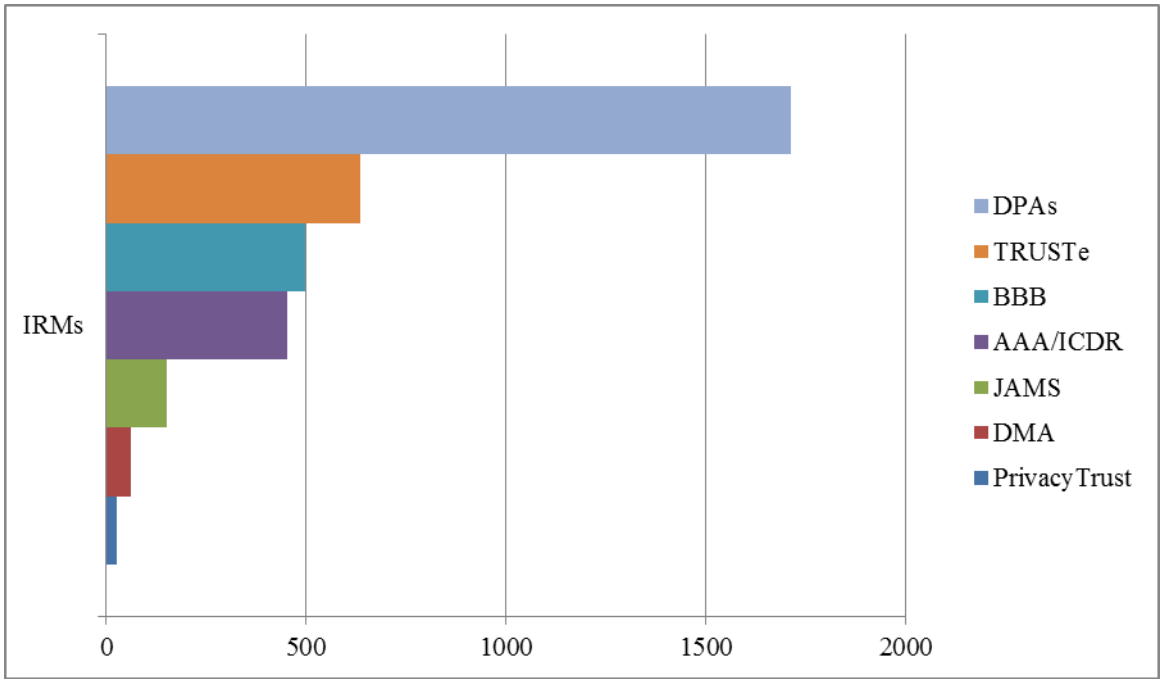
[43] Efter rapporten fra 2004 er der blevet offentliggjort en meddelelse i form af spørgsmål og svar fra EU's Databeskyttelsespanel på Kommissionens hjemmeside (Generaldirektoratet for Retlige Anliggender) for at øge borgernes kendskab til panelet og hjælpe dem med at indgive en klage, når de mener, at behandlingen af deres personoplysninger overtræder safe harbor-principperne. http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf.
Standardklageformularen kan findes på http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf.

Commissions håndhævelsesbeføjelser, må de ikke deltage i safe harbor-ordningen. Med den stigende konvergens mellem teknologier og tjenester er mange af deres direkte konkurrenter i den amerikanske IKT-sektor imidlertid medlemmer af safe harbor-ordningen. En række europæiske teleoperatører er bekymrede over, at telekommunikationsselskaberne er udelukket fra udveksling af oplysninger under safe harbor-ordningen. Ifølge European Telecommunications Network Operators' Association (ETNO) er dette "i klar modstrid med teleoperatørernes vigtigste krav, nemlig at der skal være lige vilkår for alle"[44].

6. STYRKELSE AF SAFE HARBOR-PRINCIPPERNE

6.1. Alternativ tvistbilæggelse

Princippet om håndhævelse kræver, at der skal være "**let tilgængelige og overkommelige indsigelsesprocedurer,** der gør det muligt at undersøge klager fra hver enkelt fysiske person". Til det formål indfører safe harbor-ordningen et system for alternativ tvistbilæggelse (ATB) gennem en uafhængig tredjepart[45] for at sikre fysiske personer hurtige løsninger. De tre vigtigste klageinstanser er EU's Databeskyttelsespanel, BBB (Better Business Bureaus) og TRUSTe.



Anvendelsen af ATB er steget siden 2004, og handelsministeriet har styrket overvågningen af amerikanske ATB-udbydere for at sikre, at de oplysninger, de giver om klageproceduren, er

44 "ETNO considerations", modtaget af Kommissionens tjenestegrene den 4. oktober 213, kommer også ind på 1) definitionen af personoplysninger i safe harbor-ordningen, 2) den manglende overvågning af safe harbor-ordningen og 3) det forhold, at "amerikanske virksomheder kan overføre oplysninger med meget færre begrænsninger end deres europæiske modparter", hvilket "udgør en klar forskelsbehandling af europæiske virksomheder og påvirker europæiske virksomheders konkurrenceevne". I henhold til safe harbor-reglerne må et foretagende udelukkende videregive oplysninger til tredjemand, hvis det overholder principperne om oplysningspligt og valgfrihed. Hvis et foretagende ønsker at overføre oplysninger til tredjemand, der fungerer som mellemmand, kan det gøre dette, hvis det først sikrer sig, at tredjemand overholder safe harbor-principperne, er omfattet af direktivet eller af en anden konstatering af tilstrækkelig beskyttelse, eller indgår en skriftlig aftale med tredjemand, hvormed denne forpligter sig til at sikre mindst samme beskyttelse af privatlivets fred som i de relevante principper.

45 EU's direktiv 2013/11/EU om alternativ tvistbilæggelse (ATB) i forbindelse med tvister på forbrugerområdet understreger vigtigheden af uafhængige, uvildige, gennemsigtige, effektive, hurtige og retfærdige procedurer for alternativ tvistbilæggelse.

klare, tilgængelige og forståelige. Det er dog endnu uvist, hvor effektivt systemet er, da der hidtil kun er behandlet et begrænset antal sager[46].

Selv om det er lykkedes handelsministeriet at nedbringe ATB-udbydernes gebyrer, bliver to ud af syv store ATB-udbydere ved med at kræve gebyr af fysiske personer, der indgiver en klage[47]. Disse ATB-udbydere anvendes af ca. 20 % af safe harbor-virksomhederne. Disse virksomheder har valgt en ATB-udbyder, der kræver gebyr af forbrugerne for indgivelse af en klage. Denne praksis er ikke i overensstemmelse med safe harbor-ordningens princip om håndhævelse, som giver fysiske personer ret til at få adgang til "let tilgængelige og overkommelige indsigelsesprocedurer". I Den Europæiske Union har alle registrerede gratis adgang til en uafhængig tvistbilæggelsestjeneste, som leveres af EU's Databeskyttelsespanel.

Den 12. november 2013 bekræftede handelsministeriet, at det "vil fortsætte med at gøre en indsats for EU-borgernes ret til privatlivets fred og samarbejde med ATB-udbyderne om at finde ud af, om deres gebyrer kan sænkes yderligere".

Med hensyn til sanktioner er det ikke alle ATB-udbydere, der har de nødvendige redskaber til at rette op på situationer, hvor principperne til beskyttelse af privatlivets fred ikke overholdes. Desuden ser det ikke ud til, at det er alle ATB-udbyderes sanktioner og foranstaltninger, der omfatter offentliggørelse af konstateringer af manglende overholdelse af safe harbor-principperne.

ATB-udbyderne skal også henvise sager til Federal Trade Commission, når en virksomhed ikke retter sig efter resultatet af ATB-processen eller afviser ATB-udbyderens afgørelse, så Federal Trade Commission kan gennemgå og undersøge sagen og i givet fald træffe håndhævelsesforanstaltninger. Hidtil har der dog ikke været nogen tilfælde, hvor en ATB-udbyder har henvist en sag til Federal Trade Commission på grund af manglende overholdelse af principperne[48].

Udbyderne af alternativ tvistbilæggelse har på deres hjemmesider lister over de virksomheder (deltagere i tvistbilæggelse), der anvender deres tjenester. Derved kan forbrugerne let kontrollere, om fysiske personer kan indgive en klage til en bestemt tvistbilæggelsesudbyder, hvis der opstår en tvist med en virksomhed. For eksempel har tvistbilæggelsesudbyderen BBB en liste over alle de virksomheder, som er omfattet af BBB's tvistbilæggelsessystem. Der er dog mange virksomheder, der påstår, at de er omfattet af et bestemt tvistbilæggelsessystem, men som ikke af ATB-udbyderne er opført som deltagere i deres tvistbilæggelsessystem[49].

---

46 For eksempel meddelte en af de største ATB-udbydere (TRUSTe), at den havde modtaget 881 anmodninger i 2010, men at kun tre af dem kunne behandles og var begrundede og førte til, at den pågældende virksomhed blev pålagt at ændre sit program til beskyttelse af privatlivets fred og sin hjemmeside. I 2011 indkom der 879 klager, og i ét tilfælde blev virksomheden pålagt at ændre sit program til beskyttelse af privatlivets fred. Ifølge handelsministeriet er langt de fleste klager til ATB anmodninger fra forbrugere, f.eks. brugere, der har glemt deres password og ikke har kunnet få det oplyst af internettjenesten. Handelsministeriet har på anmodning af Kommissionen udviklet nye kriterier vedrørende statistisk indrapportering, som skal anvendes af alle ATB-udbydere. De skelner mellem anmodninger og klager og giver yderligere præciseringer af, hvilke typer klager der modtages. Disse nye kriterier bør dog drøftes yderligere for at sikre, at de nye statistikker i 2014 omfatter alle ATB-udbydere, er sammenlignelige og giver oplysninger, som er afgørende for vurderingen af, hvor effektiv klagemekanismen er.

47 International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA) opkræver 200 USD og JAMS 250 USD i "klagegebyr". Handelsministeriet meddelte Kommissionen, at det havde samarbejdet med AAA, den dyreste tvistbilæggelsesudbyder for fysiske personer, om at udvikle et safe harbor-specifikt program, der nedbragte omkostningerne for forbrugerne fra flere tusinde dollars til et fast gebyr på 200 USD.

48 Se FAQ 11.

49 Eksempler: Amazon har meddelt handelsministeriet, at de anvender BBB som tvistbilæggelsesudbyder. Amazon står imidlertid ikke på BBB's liste over tvistbilæggelsesdeltagere. Omvendt står Arsalon Technologies (www.arsalon.net), en cloud hosting-tjenesteudbyder, på BBB's safe harbor-tvistbilæggelsesliste, men virksomheden er ikke et nuværende medlem af safe harbor-ordningen (situation pr. 1. oktober 2013). BBB, TRUSTe og andre ATB-udbydere bør fjerne eller rette certificeringspåstandene. De bør være pålagt et krav, der kan håndhæves, om, at de kun må certificere virksomheder, der er medlemmer af safe harbor-ordningen.

ATB-procedurerne bør være let tilgængelige og overkommelige for fysiske personer. En registreret bør kunne indgive en klage uden at støde på urimelige hindringer. Alle ATB-instanser bør på deres hjemmesider offentliggøre statistikker om de klager, de behandler, og specifikke oplysninger om resultaterne af klagerne. Endelig bør ATB-instanserne overvåges yderligere for at sikre, at de oplysninger, de giver om proceduren og om, hvordan man indgiver en klage, er klare og forståelige, så tvistbilæggelsen bliver en effektiv og troværdig procedure, der giver resultater. Det bør også gentages, at offentliggørelsen af konklusionerne om manglende overholdelse af safe harbor-principperne bør indgå i ATB-udbydernes obligatoriske sanktioner.

6.2. Videre overførsel

Med den eksponentielle stigning i datastrømmene er der behov for at sikre, at personoplysninger hele tiden beskyttes i alle faser af behandlingen af oplysninger, specielt når en virksomhed, der er medlem af safe harbor-ordningen, overfører oplysninger til en **tredjepart, der er registerfører**. Behovet for en bedre håndhævelse af safe harbor-principperne vedrører derfor ikke kun medlemmerne af safe harbor-ordningen, men også underleverandører.

Safe harbor-ordningen giver mulighed for videre overførsel af oplysninger til tredjemand, der fungerer som "mellemmand", hvis virksomheden – der er medlem af safe harbor-ordningen – "sikrer sig, at tredjemand overholder safe harbor-principperne, er omfattet af direktivet eller af en anden konstatering af tilstrækkelig beskyttelse, eller indgår en skriftlig aftale med tredjemand, hvormed denne forpligter sig til at sikre mindst samme beskyttelse af privatlivets fred som i de relevante principper"[50]. For eksempel pålægger handelsministeriet cloud-tjenesteudbydere at indgå en kontrakt, selv om de overholder safe harbor-principperne, hvis de modtager personoplysninger med henblik på behandling[51]. Denne bestemmelse er dog ikke klar i bilag II til safe harbor-beslutningen.

Da anvendelsen af underleverandører er steget betydeligt i de seneste år, specielt i forbindelse med cloud computing, bør safe harbor-virksomheder, når de indgår en sådan kontrakt, underrette handelsministeriet og være forpligtet til at offentliggøre foranstaltningerne til beskyttelse af privatlivets fred[52].

De tre ovennævnte spørgsmål, nemlig procedurer for alternativ tvistbilæggelse, øget kontrol og videre overførsel af oplysninger, bør afklares yderligere.

7. ADGANG TIL OPLYSNINGER, DER OVERFØRES INDEN FOR RAMMENE AF SAFE HARBOR-ORDNINGEN

I 2013 har oplysninger om omfanget og rækkevidden af de amerikanske overvågningsprogrammer givet anledning til bekymring over kontinuiteten i beskyttelsen af personoplysninger, der lovligt overføres til USA under safe harbor-ordningen. For eksempel ser det ud til, at alle virksomheder, der er involveret i PRISM-programmet, og som giver de

50 Se Kommissionens beslutning 2000/520/EF, side 8 (videre overførsel).

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.

52 Disse bemærkninger vedrører cloud-udbydere, som ikke er med i safe harbor-ordningen. Ifølge konsulentfirmaet Galexia "er andelen af medlemmer af safe harbor-ordningen (og overholdelsen af principperne) blandt cloud-tjenesteudbydere forholdsvis høj. Cloud-tjenesteudbydere har typisk flere lag af beskyttelse af privatlivets fred, som ofte kombinerer direkte kontrakter med kunderne og overordnede programmer til beskyttelse af privatlivets fred. Med ganske få vigtige undtagelser overholder de cloud-tjenesteudbydere, der er med i safe harbor-ordningen, de vigtigste bestemmelser vedrørende tvistbilæggelse og håndhævelse. Der er på nuværende tidspunkt ingen større cloud-tjenesteudbydere på listen over falske påstande om medlemskab". (Chris Connolly fra Galexia på et møde i LIBE-Udvalget i forbindelse med en undersøgelse om "Elektronisk masseovervågning af EU-borgere").

amerikanske myndigheder adgang til oplysninger, der lagres og behandles i USA, er safe harbor-certificerede. Det har gjort safe harbor-ordningen til en af de kanaler, hvorigennem de amerikanske efterretningsmyndigheder får adgang til at indsamle personoplysninger, der oprindelig blev behandlet i EU.

I henhold til bilag I til Safe harbor-beslutningen kan overholdelsen af principperne til beskyttelse af privatlivets fred begrænses, hvis det er nødvendigt af hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden eller af love, administrative bestemmelser eller retspraksis. Begrænsninger af udøvelsen af de grundlæggende rettigheder er kun gyldige, hvis de fortolkes snævert; de skal være fastsat i en offentligt tilgængelig lov og skal være nødvendige og rimelige i et demokratisk samfund. Det præciseres specielt i safe harbor-beslutningen, at sådanne begrænsninger kun er tilladt, hvis de er **"begrænset til et niveau, der er tilstrækkeligt"** for at opfylde kravene med hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden[53]. Safe harbor-ordningen giver ganske vist mulighed for undtagelsesvis behandling af oplysninger med henblik på statens sikkerhed, almenvellet eller opretholdelse af lov og orden, men på det tidspunkt, hvor safe harbor-beslutningen blev vedtaget, kunne man ikke forudse efterretningstjenesternes storstilede adgang til oplysninger, der overføres til USA i forbindelse med handelstransaktioner.

Af hensyn til gennemsigtigheden og retssikkerheden bør handelsministeriet desuden underrette Europa-Kommissionen om alle love og administrative bestemmelser, der kan påvirke overholdelsen af safe harbor-principperne[54]. Anvendelsen af undtagelser bør overvåges øje, og undtagelserne må ikke bruges på en måde, der underminerer den beskyttelse, som **principperne** giver[55]. Specielt risikerer de amerikanske myndigheders storstilede adgang til oplysninger, som behandles af virksomheder, der har foretaget safe harbor-selvcertificering, at undergrave den elektroniske kommunikations fortrolighed.

7.1. Proportionalitet og nødvendighed

Som det fremgår af resultaterne af arbejdet i ad hoc-gruppen mellem EU og USA om databeskyttelse, tillader en række retsgrundlag i amerikansk ret storstilet indsamling og behandling af personoplysninger, der lagres eller på anden måde behandles af virksomheder i USA. Der kan bl.a. være tale om oplysninger, som tidligere er blevet overført fra EU til USA under safe harbor-ordningen, hvilket rejser spørgsmålet om, hvorvidt safe harbor-principperne stadig overholdes. Fordi disse programmer er så omfattende, kan det medføre, at de amerikanske myndigheder får adgang til og viderebehandler oplysninger, der er overført under safe harbor-ordningen, ud over hvad der er strengt nødvendigt og proportionalt i forhold til beskyttelsen af statens sikkerhed, jf. undtagelsen i safe harbor-beslutningen.

---

53 Se bilag I til safe harbor-beslutningen: "Overholdelsen af disse principper kan være begrænset a) til et niveau, der er tilstrækkeligt for at opfylde kravene med hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden, b) af love, administrative bestemmelser eller retspraksis, der medfører modstridende forpligtelser eller udtrykkelige tilladelser, såfremt foretagender i forbindelse med anvendelsen af sådanne tilladelser kan påvise, at de kun overtræder principperne i det omfang, som er nødvendigt for at tilgodese de altovervejende legitime interesser, som den pågældende tilladelse har til hensigt at fremme, eller c) i det omfang, direktivet eller medlemsstaternes lovgivning tillader undtagelser eller dispensationer, såfremt sådanne undtagelser eller dispensationer også finder anvendelse i sammenlignelig kontekst. I overensstemmelse med det overordnede mål om at fremme beskyttelsen af privatlivets fred bør foretagenderne bestræbe sig på at gennemføre disse principper på fuldstændig og gennemskuelig vis, hvilket omfatter, at de i deres program til beskyttelse af privatlivets fred angiver, på hvilke punkter eventuelle undtagelser fra principperne i henhold til ovenstående punkt b) finder generel anvendelse. Når principperne og/eller den amerikanske lovgivning giver mulighed derfor, forventes foretagenderne af samme årsag at vælge et højere beskyttelsesniveau."

54 Udtalelse 4/2000 om det beskyttelsesniveau, der opnås ved hjælp af safe harbor-principperne, vedtaget af Artikel 29-Gruppen vedrørende Databeskyttelse den 16. maj 2000.

55 Udtalelse 4/2000 om det beskyttelsesniveau, der opnås ved hjælp af safe harbor-principperne, vedtaget af Artikel 29-Gruppen vedrørende Databeskyttelse den 16. maj 2000.

7.2. Begrænsninger og klagemuligheder

Som det fremgår af resultaterne af arbejdet i ad hoc-gruppen mellem EU og USA om databeskyttelse, gælder de sikkerhedsforanstaltninger, som findes i henhold til amerikansk ret, for det meste for amerikanske statsborgere eller personer med lovligt ophold. Desuden har hverken registrerede i EU eller i USA mulighed for at opnå indsigt i eller berigtigelse eller sletning af oplysninger eller administrativ eller retslig prøvelse med hensyn til den indsamling og viderebehandling af deres personoplysninger, der finder sted som led i de amerikanske overvågningsprogrammer.

7.3. Gennemsigtighed

Virksomhederne angiver ikke systematisk i deres programmer til beskyttelse af privatlivets fred, hvornår de anvender undtagelser til principperne. Hverken fysiske personer eller virksomheder ved således, hvad de sker med deres oplysninger. Det er særlig relevant i forbindelse med de pågældende amerikanske overvågningsprogrammer. Det betyder, at virksomhederne ikke gør europæere, hvis oplysninger overføres til en virksomhed i USA under safe harbor-ordningen, opmærksom på, at der kan gives adgang til deres oplysninger[56]. Det rejser spørgsmålet om overholdelsen af safe harbor-principperne om gennemsigtighed. Gennemsigtigheden bør sikres i videst muligt omfang, uden at statens sikkerhed bringes i fare. Ud over de eksisterende krav om, at virksomhederne bør oplyse det i deres program til beskyttelse af privatlivets fred, når principperne kan være begrænset af love, administrative bestemmelser eller retspraksis, bør de også tilskyndes til at oplyse det i deres program til beskyttelse af privatlivets fred, når de anvender undtagelser fra principperne for at opfylde kravene med hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden.

8. KONKLUSIONER OG ANBEFALINGER

Siden vedtagelsen i 2000 er safe harbor-ordningen blevet et redskab for strømme af personoplysninger mellem EU og USA. Betydningen af en effektiv beskyttelse i forbindelse med overførsel af personoplysninger er steget på grund af den eksponentielle vækst i datastrømmene, som er en afgørende del af den digitale økonomi, og den meget store stigning i indsamlingen, behandlingen og anvendelsen af oplysninger. Webvirksomheder som Google, Facebook, Microsoft, Apple og Yahoo har hundreder af millioner af kunder i Europa og overfører personoplysninger med henblik på behandling til USA i et omfang, som man ikke kunne forestille sig i 2000, da safe harbor-ordningen blev indført.

På grund af mangler i gennemsigtigheden og håndhævelsen af ordningen er der stadig en række specifikke problemer, som der må gøres noget ved:

a) gennemsigtigheden af safe harbor-medlemmernes programmer til beskyttelse af privatlivets fred

b) en effektiv anvendelse af principperne til beskyttelse af privatlivets fred i virksomheder i USA og

c) en effektiv håndhævelse.

[56] En række europæiske virksomheder, som er med i safe harbor-ordningen, giver forholdsvis gennemsigtige oplysninger på dette område. For eksempel giver Nokia, der har aktiviteter i USA og er medlem af safe harbor-ordningen, følgende oplysninger i sit program til beskyttelse af privatlivets fred: *"Der kan være tilfælde, hvor vi efter loven har pligt til at videregive dine personoplysninger til visse myndigheder eller anden tredjemand, f.eks. politimyndigheder i lande, hvor vi eller nogen tredjemand handlende på vores vegne har aktiviteter."*

Desuden rejser **efterretningstjenesternes omfattende adgang til oplysninger, som safe harbor-certificerede virksomheder har overført til USA**, yderligere alvorlige spørgsmål vedrørende kontinuiteten i europæernes databeskyttelsesrettigheder, når deres oplysninger overføres til USA.

På grundlag af ovenstående fremsætter Kommissionen følgende **anbefalinger**:

Gennemsigtighed

1. *Selvcertificerede virksomheder bør offentliggøre deres programmer til beskyttelse af privatlivets fred.* Det er ikke nok, at virksomhederne sender handelsministeriet en beskrivelse af deres program. Programmerne bør være offentligt tilgængelige på virksomhedernes hjemmesider på et klart og letforståeligt sprog.
2. *Selvcertificerede virksomheders hjemmesider bør altid omfatte et link til handelsministeriets safe harbor-hjemmeside, som indeholder en liste over alle "nuværende" medlemmer af ordningen.* Det vil gøre det muligt for registrerede i Europa med det samme at kontrollere, om en virksomhed på nuværende tidspunkt er medlem af safe harbor-ordningen, uden at de behøver at foretage yderligere søgninger. Det vil være med til at øge ordningens troværdighed ved at mindske mulighederne for falske påstande om medlemskab af safe harbor-ordningen. Handelsministeriet begyndte i marts 2013 at stille dette krav til virksomhederne, men processen bør intensiveres.
3. *Selvcertificerede virksomheder bør offentliggøre de bestemmelser til beskyttelse af privatlivets fred, der indgår i alle kontrakter, som de indgår med underleverandører, f.eks. cloud computing-tjenester.* Safe harbor-ordningen giver mulighed for videre overførsel fra virksomheder, der har foretaget safe harbor-selvcertificering, til tredjemand, der fungerer som "mellemmand", for eksempel til cloud-tjenesteudbydere. Efter vores opfattelse kræver handelsministeriet i sådanne tilfælde, at de selvcertificerede virksomheder indgår en kontrakt. Når safe harbor-virksomheder indgår en sådan kontrakt, bør de imidlertid underrette handelsministeriet og være forpligtet til at offentliggøre foranstaltningerne til beskyttelse af privatlivets fred.
4. *Alle virksomheder, der ikke er nuværende medlemmer af ordningen, bør klart markeres på handelsministeriets hjemmeside.* Angivelsen "ikke nuværende" på handelsministeriets liste over safe harbor-medlemmer bør ledsages af en klar advarsel om, at en virksomhed ikke på nuværende tidspunkt opfylder safe harbor-kravene. "Ikke nuværende" virksomheder er dog forpligtet til fortsat at anvende safe harbor-kravene på de oplysninger, de har modtaget under safe harbor-ordningen.

Klageadgang

5. *Programmerne til beskyttelse af privatlivets fred på virksomhedernes hjemmesider bør omfatte et link til instansen for alternativ tvistbilæggelse (ATB) og/eller EU-Panelet.* Det vil gøre det muligt for registrerede i Europa straks at kontakte ATB-instansen eller EU-Panelet, hvis der opstår problemer. Handelsministeriet begyndte i marts 2013 at stille dette krav til virksomhederne, men processen bør intensiveres.
6. *Alternativ tvistbilæggelse bør være let tilgængelig og økonomisk overkommelig.* Nogle ATB-instanser i safe harbor-ordningen opkræver stadig gebyr af fysiske personer – hvilket kan være ganske dyrt for almindelige brugere – for behandling af klagen (200-

250 USD). Derimod er der i Europa gratis adgang til Databeskyttelsespanelet, som har til opgave at behandle klager under safe harbor-ordningen.

7. *Handelsministeriet bør mere systematisk overvåge ATB-instanserne med hensyn til gennemsigtigheden og tilgængeligheden af de oplysninger, de giver om den procedure, de anvender, og deres opfølgning af klager.* Det gør tvistbilæggelse til en effektiv og pålidelig mekanisme, som giver resultater. Det bør også gentages, at offentliggørelsen af konklusionerne om manglende overholdelse af safe harbor-principperne bør indgå i ATB-udbydernes obligatoriske sanktioner.

Håndhævelse

8. *Efter certificeringen eller recertificeringen af virksomheder under safe harbor-ordningen bør en vis procentdel af disse virksomheder underkastes ex officio-undersøgelser af, om de effektivt overholder deres programmer til beskyttelse af privatlivets fred (undersøgelserne bør omfatte mere end blot en kontrol af, om de formelle krav overholdes*).

9. *Når det efter en klage eller en undersøgelse er konstateret, at en virksomhed ikke overholder kravene, bør virksomheden underkastes en opfølgende specifik undersøgelse efter et år.*

10. *Hvis der er tvivl om, hvorvidt en virksomhed overholder kravene, eller hvis der er indgivet klager, bør handelsministeriet underrette den kompetente EU-databeskyttelsesmyndighed.*

11. *Falske påstande om medlemskab af safe harbor-ordningen bør fortsat efterforskes.* En virksomhed, der på sin hjemmeside påstår, at den overholder safe harbor-kravene, men som ikke er opført på handelsministeriets liste over "nuværende" medlemmer af ordningen, vildleder forbrugerne og misbruger deres tillid. Falske påstande svækker hele systemets troværdighed og bør derfor øjeblikkelig fjernes fra virksomhedernes hjemmesider.

De amerikanske myndighedes adgang til oplysninger

12. *Selvcertificerede virksomheders programmer til beskyttelse af privatlivets fred bør omfatte oplysninger om, i hvilket omfang den amerikanske lovgivning giver offentlige myndigheder mulighed for at indsamle og behandle oplysninger, der er blevet overført under safe harbor-ordningen. Specielt bør virksomhederne tilskyndes til at angive det i deres programmer, når de anvender undtagelser til principperne for at opfylde kravene med hensyn til statens sikkerhed, almenvellet eller opretholdelsen af lov og orden.*

13. *Det er vigtigt, at den undtagelse vedrørende statens sikkerhed, som findes i safe harbor-beslutningen, kun anvendes, når det er strengt nødvendigt eller proportionalt.*