Folketinget — Europaudvalget
Christiansborg, den 28. juni 2007
EU-konsulenten

Til

udvalgets medlemmer og stedfortrædere

Baggrundsnote om SWIFT-sagen

Resumé

Som led i terrorbekæmpelsen har de amerikanske myndigheder i strid med EU's persondatadirektiv fået udleveret personoplysninger fra det såkaldte SWIFT-system, som behandler internationale pengetransaktioner. Oplysningerne hidrører fra SWIFT-netværkets database i USA, som indeholder samtlige elektroniske oplysninger i det verdensomspændende SWIFT-system. På den baggrund har EU og USA arbejdet på at finde en løsning, som sikrer, at udlevering af data fremover kan ske på en måde, der er forenelig med EU-reglerne.

Baggrund

Efter terrorangrebene i september 2001 søgte de amerikanske myndigheder adgang til personoplysninger vedrørende pengetransaktioner fra den såkaldte SWIFT-database, der befinder sig på USA's område. SWIFT-databasen indeholder oplysninger om alle pengetransaktioner foretaget i det såkaldte SWIFT-system, herunder oplysninger om transaktioner mellem EU-lande og mellem EU-lande og tredjelande. Myndighederne fik på baggrund af amerikanske retskendelser udleveret oplysninger så som navne på indbetalere og modtagere, hvilke er oplysninger, som er omfattet af EU's persondatadirektiv[1].

Det belgiske finanstilsyn og en uafhængig EU-arbejdsgruppe fastslog efter-

[1] Europa-Parlamentet og Rådets 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 (*EFT L 281 af 23.11.1995, s. 31).*

følgende, at udleveringen af data fra SWIFT-systemet ikke levede op til direktivets krav.

På den baggrund er Kommissionen gået i dialog med de amerikanske myndigheder med henblik på at finde en løsning, der sikrer, at evt. udlevering af data fra SWIFT kan ske på en måde, der er forenelig med EU-reglerne.

Hvad er SWIFT?

SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) er et internationalt finansielt netværk, der formidler internationale pengeoverførsler. SWIFT er stiftet som et aktieselskab med hovedsæde i Belgien og driftskontorer i bl.a. Nederlandene og USA, som ejes af ca. 3000 finansielle virksomheder med omkring 8000 forretningsenheder fordelt på 205 lande. Alle dataoplysninger vedrørende SWIFT-transaktioner opbevares i 124 dage og lagres af sikkerhedsgrunde i to databaser, én i Nederlandene, én i USA (også kaldet "spejling"). Således indeholder databasen i USA også oplysninger om betalingsoverførsler mellem EU-landene og mellem EU og resten af verden.

De oplysninger, som lagres i SWIFT-databaserne, vil således typisk være navne og adresser på personer, der afsender eller modtager pengeoverførsler, oplysninger om tidspunkter for overførsler, kontonumre og lign.

For så vidt angår den praktiske håndtering af anmodninger fra de amerikanske myndigheder har SWIFT oplyst[2],

- at de amerikanske myndigheder kun har adgang til en begrænset del af oplysningerne i databasen,
- at der for hver gang, der gives oplysninger, foreligger en kendelse,
- at aktuelle søgninger finder sted på grundlag af de faktiske oplysninger, der danner grundlag for kendelsen,
- at SWIFT ikke selv har kendskab til, hvilke konkrete transaktioner søgningen i den enkelte sag viser og derfor ikke kan svare på, om der har været udleveret oplysninger om transaktioner, hvor danske kunder er involveret,
- at der kun i begrænset omfang er givet mulighed for adgang til oplysninger om nationale overførsler i de europæiske lande,

[2] Jf. skrivelse af 4. august 2006 fra Finanstilsynet som svar på spørgsmål Nr. S 5823 af 27. juni 2006 om adgangen til SWIFT-databasen.

- at man aldrig udleverer oplysninger uden, at der foreligger et juridisk holdbart grundlag.

Persondatadirektivet
Persondatadirektivet har til formål at sikre beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder, især retten til privatlivets fred, i forbindelse med behandling af personoplysninger. Direktivet opstiller bl.a. reglerne for udlevering af personoplysninger fra elektroniske registre.

Eftersom SWIFT har hjemsted i Belgien, var det i første omgang det belgiske datatilsyn, der konstaterede, at udleveringen af oplysninger til de amerikanske myndigheder var i konflikt med EU-reglerne. Senere blev sagen også taget op af en uafhængig arbejdsgruppe nedsat af EU i henhold til databeskyttelsesdirektivets artikel 29 (kaldet artikel 29-arbejdsgruppen). Begge instanser når frem til, at SWIFT's videregivelse af oplysninger fra databasen i USA ikke overholdt kravene i persondatadirektivet.

I sin udtalelse af 22. november 2006[3] fastslår artikel 29-arbejdsgruppen bl.a., at udleveringen af oplysningerne er sket i strid med direktivets regler, herunder:

- **Kravet om anvendelse til forenelige formål** (direktivets artikel 6, stk. 1, litra b): Personoplysninger må kun benyttes til formål, der er forenelige med det oprindelige formål med indsamlingen af oplysningerne. Rapporten fastslår, at behandlingen af personoplysninger med henblik på efterforskning af påstået terrorisme ikke er forenelig med det oprindelige formål med indsamlingen af personoplysninger, som udelukkende var erhvervsmæssigt.

- **Oplysningspligten** (direktivets artikel 10 og 11)**:** Den registrerede person skal underrettes om behandlingen af dennes personoplysninger og om overførslen til USA. Arbejdsgruppen anfører, at alle kunder i pengeinstitutter uanset deres nationalitet eller hjemland har ret til at få at vide, hvad der sker med deres "fortrolige" data, og konkluderer, at hverken SWIFT eller pengeinstitutterne i EU har givet informationer til registrerede personer om behandlingen af deres personoplysninger og navnlig om overførslen til USA.

[3] Udtalelsen (10/2006) kan findes på Kommissionens hjemmeside: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_da.pdf

- **Anmeldelsespligten** (direktivets artikel 18–20)**:** De registeransvarlige skal anmelde deres databehandlingsaktiviteter til eller sikre forudgående kontrol hos de nationale datatilsynsmyndigheder. Gruppen bemærker i den forbindelse, at SWIFT faktisk anmeldte visse typer databehandling til det belgiske datatilsyn, men at det ikke anmeldte behandlingen og spejlingen i driftscentret i USA til udførelse af internationale betalingsordrer og heller ikke det senere formål.

- **Kravet om tilstrækkeligt beskyttelsesniveau** (direktivets artikel 25 og 26): Videregivelse af data, der er genereret i EU, og som skal bruges uden for EU, skal underkastes en vurdering af, om beskyttelsesniveauet er tilstrækkeligt i henhold til direktivet. Gruppen fastslår bl.a., at dette krav ikke er blevet overholdt i forbindelse med udleveringen, og at SWIFT ikke udnyttede mekanismerne i direktivet til at opnå tilladelse fra det belgiske datatilsyn til behandlingsaktiviteterne.

- **Kravet om passende kontrolmekanismer** (direktivets artikel 28): De offentlige datatilsynsmyndigheder skal kunne iværksætte en uafhængig kontrol, hvilket forudsætter, at videregivelsen anmeldes til myndighederne. Arbejdsgruppen fastslår, at selv om SWIFT fastsatte nogle kontrolforanstaltninger, navnlig vedrørende det amerikanske handelsministeriums adgang til oplysningerne, erstatter disse på ingen måde tilsynsmyndighedernes uafhængige granskning.

Proceduren ved konstatering af utilstrækkeligt beskyttelse
I henhold til persondatadirektivet (artikel 25, stk. 4 og 5), skal Kommissionen, når den konstaterer, at et tredjelands regler ikke sikrer et passende beskyttelsesniveau med hensyn til beskyttelse af personoplysninger, indlede forhandlinger med henblik på at afhjælpe denne situation.

Kommissionen kan herefter, på grundlag af en samlet vurdering - herunder navnlig af oplysningernes art, de påtænkte behandlingers formål og varighed, oprindelseslandet og det endelige bestemmelsesland, retsreglerne i det pågældende tredjeland, samt landets regler for god forretningsskik og sikkerhedsforanstaltninger - fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau med henblik på at beskytte privatlivet og personers grundlæggende rettigheder og frihedsrettigheder[4].

[4] Jf. direktivets artikel 25, stk. 6. Beslutningen træffes efter en komitologiprocedure (forskriftsprocedure) hvor Kommissionen bistås af embedsmænd fra medlemsstaterne.

Safe harbor-ordningen

Safe harbor-ordningen er udviklet af USA's handelsministerium i samarbejde med Kommissionen, og indebærer, at foretagender, som ønsker at videresende oplysninger omfattet af EU's databeskyttelsesdirektiv, skal tilslutte sig "*safe harbor*-principperne" (jf. kassen nedenfor). Disse foretagender opføres på en liste, som offentliggøres på USA's handelsministeriums hjemmeside.

Kommissionen fastslog i sin beslutning af 26. juli 2000, at *safe harbor*-ordningen sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra EU til foretagender etableret i USA[5].

Ifølge regeringens supplerende samlenotat om SWIFT-sagen[6] har Kommissionen vurderet, at overførsel af data til SWIFT-databasen i USA kan ske inden for direktivets rammer, hvis SWIFT tilslutter sig *safe harbor*-ordningen, hvilket SWIFT har besluttet sig at gøre.

Safe harbor-principperne [7]

Oplysningspligt: Et foretagende skal oplyse fysiske personer om, hvilke formål der ligger til grund for indsamlingen og anvendelsen af personoplysninger om de pågældende, hvorledes foretagendet kan kontaktes i tilfælde af valgmuligheder og midler foretagendet tilbyder disse fysiske personer med henblik på at begrænse anvendelsen eller videregivelsen af personoplysninger.

[5] Jf. artikel 1 i Kommissionens beslutning 2000/520/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).

[6] Jf. regeringens supplerende samlenotat - EUU Alm. Del. – bilag 388.

[7] Den fulde beskrivelse af Safe Harbor-principperne findes i bilag I til Kommissionens beslutning 2000/520/EF – se fodnote 5, samt på USA's handelsministeriums hjemmeside: http://www.export.gov/safeharbor/sh_overview.html

Valgfrihed: Et foretagende skal give fysiske personer mulighed for at vælge (opt out), hvorvidt deres personoplysninger skal a) videregives til tredjemand eller b) anvendes til et formål, der er uforeneligt med det, hvortil personoplysningerne oprindeligt blev indsamlet. I tilfælde af følsomme oplysninger (dvs. personoplysninger om helbredsforhold, race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmedlemsskab eller oplysninger om seksuelle forhold) skal de pågældende fysiske personer udtrykkeligt give deres godkendelse (opt in), hvis oplysningerne skal videregives til tredjemand eller anvendes til et andet formål end det, hvortil de oprindeligt er blevet indsamlet.

Videre overførsel: Et foretagende må udelukkende videregive personoplysninger til tredjemand, hvis det overholder principperne om oplysningspligt og valgfrihed. Hvis foretagendet ønsker at overføre oplysninger til tredjemand, der fungerer som mellemmand, skal det først sikre 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 principperne.

Sikkerhed: Et foretagende, der opretter, vedligeholder, anvender eller spreder personoplysninger, skal træffe passende foranstaltninger for at beskytte disse oplysninger mod tab, misbrug, uautoriseret adgang, videregivelse, ændring eller ødelæggelse.

Dataintegritet: Personoplysninger skal være relevante i forhold til det formål, hvortil de anvendes. Et foretagende må ikke behandle personoplysninger på en måde, der ikke er i overensstemmelse med det formål, hvortil de oprindeligt er blevet indsamlet. Et foretagende skal i det omfang, det er nødvendigt, træffe passende foranstaltninger for at sikre, at oplysningerne er pålidelige, nøjagtige, fuldstændige og ajourførte.

Indsigt: Fysiske personer skal have adgang til de personoplysninger, som et foretagende er i besiddelse af om dem, og de skal have mulighed for at ændre eller fjerne ukorrekte oplysninger, medmindre arbejdet eller omkostningerne ved at give indsigt i det enkelte tilfælde er uforholdsmæssig store i forhold til risikoen for disse fysiske personers privatliv, eller medmindre andre fysiske personers rettigheder herved krænkes

Håndhævelse: En effektiv beskyttelse af privatlivets fred forudsætter en række mekanismer til at sikre, at safe harbor-principperne overholdes, at de fysiske personer, som personoplysningerne vedrører, kan gøre indsigelse, hvis principperne ikke overholdes, og at det får konsekvenser for et foretagende, hvis det ikke overholder principperne. Disse mekanismer skal som minimum omfatte:
a) let tilgængelige, overkommelige og uafhængige indsigelsesprocedurer,
b) kontrolprocedurer med henblik på at undersøge, om et foretagender lever op til de erklæringer og løfter, det har afgivet

c) en forpligtelse til at afhjælpe eventuelle problemer, hvis et foretagende ikke overholder principperne, samt passende sanktionsbestemmelser.

Mulighed for at fravige safe harbor-principperne
Regeringen har i sit supplerende samlenotat oplyst, at det er en del af *safe harbor*-principperne, at disse kan fraviges i det omfang det er nødvendigt for at imødekomme visse samfundsmæssige hensyn som for eksempel hensynet til national sikkerhed, hensynet til offentligheden eller krav i forbindelse med retsforfølgning. Fravigelse af principperne kan imidlertid kun ske, hvis **proportionalitetsprincippet** er overholdt.

Til brug for vurderingen af, om fravigelse af *safe harbor*-reglerne opfylder kravet om proportionalitet, vil USA afgive en **erklæring**, som blandt andet vil indeholde:
- en garanti for, at oplysningerne vil blive anvendt til terrorbekæmpelse,
- vilkår for videregivelse til andre amerikanske myndigheder,
- begrænsning af anvendelse til de nødvendige data,
- maksimumgrænser for hvor længe oplysningerne kan opbevares
- mulighed for overvågning og kontrol for EU.

En sådan erklæring vil ifølge Kommissionen opfylde betingelserne for, at SWIFT's udlevering af oplysninger fra sin database i USA kan anses for at være nødvendig og proportional og dermed er i overensstemmelse med *safe harbor*-principperne og direktivet. Kommissionen og formandskabet forventes at udpege en **europæisk kontaktperson** til at overvåge overholdelsen af erklæringen.

Ifølge regeringens samlenotat har Rådets juridiske tjeneste udtalt, at den valgte fremgangsmåde er tilstrækkelig, dels fordi EU ikke påtager sig forpligtelser overfor USA, dels fordi eventuelle ændringer i de amerikanske myndigheders behandling af oplysninger fra SWIFT's database i USA kan imødegås ved passende tiltag fra EU's side herunder et muligt krav fra EU's datatilsynsmyndigheder om at standse anvendelsen af safe harbor-løsningen i relation til SWIFT.

Sagens behandling i Folketinget
Sagen blev forelagt Europaudvalget til orientering den 23. juni 2007 med henblik på vedtagelse som a-punkt på rådsmødet (miljø) den 26. juni 2007. Sagen har tidligere været nævnt på Europaudvalgets møde den 24. november 2006 og har været genstand for spørgsmål 2766 af 24. november 2006 samt spørgsmål Nr. S 5823 af 27. juni 2006.

Med venlig hilsen

Thomas Fich
(3611)