EUROPA-
KOMMISSIONEN

Bruxelles, den 27.11.2013
COM(2013) 842 final

MEDDELELSE FRA KOMMISSIONEN EDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Et europæisk system til sporing af finansiering af terrorisme (EU-TFTS)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

MEDDELELSE FRA KOMMISSIONEN EDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Et europæisk system til sporing af finansiering af terrorisme (EU-TFTS)

Formålet med denne meddelelse er - som opfølgning på meddelelsen af 13. juli 2011 (KOM(2011) 429) - at informere Europa-Parlamentet og Rådet om resultaterne af analysen af, hvorvidt det kan lade sig gøre at indføre et europæisk system til sporing af finansiering af terrorisme (EU-TFTS).

1. BAGGRUND

1.1. Baggrund for anmodningen og definitioner

I løbet af de forhandlinger, der fik forud for indgåelsen af TFTP-aftalen mellem EU og USA[1], blev det drøftet, hvorledes personoplysninger og grundlæggende rettigheder kan beskyttes på bedste vis inden for rammerne af denne aftale. Visse parter fremførte, at udtrækning af data på europæisk område vil begrænse den mængde data, der overføres til USA, og dermed sikre en højere grad af sikkerhed for databeskyttelse. Nogle medlemsstater så en fordel i på længere sigt at udvikle et uafhængigt europæisk system til sporing af finansiering af terrorisme. Europa-Parlamentet anmodede Rådet og Kommissionen om at træffe alle nødvendige foranstaltninger for at udarbejde en varig, juridisk forsvarlig europæisk løsning på spørgsmålet om udtrækning af data, der er anmodet om, på europæisk område. Da Rådet og Europa-Parlamentet indgik TFTP-aftalen mellem EU og USA, blev Kommissionen anmodet om inden for et år fra datoen for aftalens ikrafttræden at fastlægge en juridisk og teknisk ramme for udtrækning af data på europæisk område og inden for tre år fra datoen for aftalens ikrafttræden at fremlægge en statusrapport om udviklingen af et tilsvarende EU-system[2]. Det anføres desuden i artikel 11 i TFTP-aftalen mellem EU og USA, at Kommissionen i aftalens løbetid vil foretage en undersøgelse af, om det er muligt at indføre et tilsvarende EU-system, der gør det muligt at sikre en mere målrettet overførsel af data.

I denne meddelelse skelnes der mellem et tilsvarende EU-system og en ramme for udtrækning af data på europæisk område. En *ramme for udtrækning af data* på europæisk område skal forstås som et system, der gør det muligt, at søgninger i data, som EU for øjeblikket stiller til

[1] EUT L 195 af 27.7.2010, s. 5.
[2] Rådets afgørelse af 13. juli 2010 (EUT L 195 af 27.7.2010, s. 3).

rådighed for USA, kan foregå på europæisk område. Et *tilsvarende EU-system* er derimod et uafhængigt europæisk system til sporing af finansiering af terrorisme gennem adgang til, søgninger i og analyse af data fra en eller flere udpegede udbydere. Indførelse af et EU-system vil kræve en ændring af TFTP-aftalen mellem EU og USA.

1.2. Hidtidige tiltag

I december 2010 lod Kommissionen foretage en *undersøgelse*, som i juli 2011 blev udvidet til også at omfatte den yderligere mulighed at indføre et lagrings- og udtrækningssystem. Kommissionen afholdt i forbindelse med undersøgelsen fire ekspertmøder med interessenter såsom Europol, Den Europæiske Tilsynsførende for Databeskyttelse, den i TFTP-aftalen udpegede udbyder[3] og flere eksperter fra medlemsstaterne, som repræsenterede berørte ministerier, retshåndhævende myndigheder og efterretningstjenester samt databeskyttelsesmyndigheder.

Den 13. juli 2011 fremlagde Kommissionen i sin *meddelelse til Europa-Parlamentet og Rådet* ("2011-meddelelsen") fem løsninger for indførelse af et europæisk system til sporing af finansiering af terrorisme ("EU-TFTS"). Det blev vurderet, at tre af disse ville kunne gennemføres. Målet med 2011-meddelelsen var at skabe debat om det videre forløb og bidrage til den efterfølgende konsekvensanalyse.

Spørgsmålet blev i oktober 2011 fremlagt for Rådet (retlige og indre anliggender) og Europa-Parlamentets Udvalg om Borgernes Rettigheder.

Eftersom medlemsstaterne og Europa-Parlamentet ikke udtrykte en klar præference for nogen af løsningerne, blev det besluttet at se på dem alle i Kommissionens konsekvensanalyse og uddybe dem ved at udvikle forskellige delløsninger. Nærværende meddelelse bygger på konsekvensanalysen[4].

[3] Society for Worldwide Interbank Financial Telecommunication (SWIFT).
[4] SWD 2013 (xx) af …

2. KOMMISSIONENS KERNEPRINCIPPER OG LØSNINGER

2.1. Principper i informationsstyringsstrategien vedtaget under det svenske formandsskab

I sin analyse om det foreslåede videre forløb tager Kommissionen hensyn til de kerneprincipper, der blev fastsat i informationsstyringsstrategien fra 2009[5] og senere integreret og udviklet i Kommissionens meddelelser om en oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed[6] og meddelelsen fra 2012 om den europæiske informationsudvekslingsmodel[7].

Det altafgørende er i den henseende principperne om beskyttelse af grundlæggende rettigheder, nødvendighed, proportionalitet og omkostningseffektivitet.

Beskyttelse af *grundlæggende rettigheder* som forankret i Den Europæiske Unions charter om grundlæggende rettigheder, navnlig retten til respekt for privatliv og beskyttelse af personoplysninger, er en prioritet for Kommissionen i forbindelse med udarbejdelse af nye forslag, der indebærer behandling af personoplysninger på området intern sikkerhed. Chartrets artikel 7 og 8 bestemmer, at "Enhver har ret til respekt for sit privatliv og familieliv" og til "beskyttelse af personoplysninger, der vedrører ham/hende". Artikel 16 i traktaten om Den Europæiske Unions funktionsmåde, som er bindende for medlemsstaterne, EU-institutionerne, agenturer og organer, fastslår, at enhver har ret til "beskyttelse af personoplysninger om vedkommende selv". Ifølge chartrets artikel 52 kan der under iagttagelse af proportionalitetsprincippet kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder.

Indgreb i retten til privatlivets fred betragtes som *nødvendig*, hvis det skyldes et presserende behov, hvis det står i et rimeligt forhold til det forfulgte mål, og hvis de grunde, den offentlige myndighed anfører som begrundelse, er relevante og tilstrækkelige.

Selvom det er vanskeligt at vurdere de finansielle omkostninger ved terrorisme, består princippet om *omkostningseffektivitet* fortsat. En *omkostningseffektiv* tilgang tager højde for

[5] Rådets konklusioner af 30. november 2009 om en informationsstyringsstrategi for EU's indre sikkerhed 16637/09.
[6] KOM(2010)385 af 20. juli 2010.
[7] KOM(2012) 735 af 7. december 2012

allerede eksisterende løsninger med henblik på at mindske overlapning og øge mulige synergier. Det er nødvendigt at vurdere, om det er muligt at opfylde et forslags målsætninger gennem bedre brug af allerede eksisterende instrumenter.

2.2. Tilgang

Kommissionen har på baggrund af førnævnte principper undersøgt, hvorvidt et EU-TFTS - sammenlignet med den nuværende situation - vil være nødvendigt og stå i et rimeligt forhold til omkostningerne, fordelene og konsekvenserne for de grundlæggende rettigheder.

Hvad angår *fordelene* vil et EU-system øge EU's og medlemsstaternes mulighed for at få adgang til relevante oplysninger og styrke deres analytiske kapaciteter med hensyn til at spore og identificere terrorister via finansielle transaktioner. Eftersom finansielle transaktioner kan give værdifulde efterretninger, som måske ikke er tilgængelige via andre kilder, vil dette værktøj være særlig nyttigt til sporing af terroristaktiviteter og involverede parter. EU-TFTS vil derfor kunne udgøre et supplerende efterretnings- og efterforskningsværktøj i kampen mod terrorisme og medføre en forøgelse af sikkerheden i EU, navnlig hvis et sådant system kunne omfatte flere udbydere af finansielle data og transaktionstyper. Fordelene ved EU-TFTS skal afvejes i forhold til de forventede omkostninger ved indførelse og vedligholdelse af systemet, herunder den finansielle byrde for medlemsstaterne og de berørte udpegede dataudbydere.

2.3. Præsentation af løsningerne

Der er overvejet flere løsninger såvel for *en ramme for udtræk af data* på EU's område som for *et tilsvarende EU-system*.

2.3.1. En ramme for udtrækning af data på EU's område

En ramme for udtrækning af data på EU's område vil kunne indføres gennem et lagrings- og udtrækningssystem for data fra den udpegede udbyder ved at tillade direkte adgang til data, som i øjeblikket stilles til rådighed for USA under TFTP-aftalen. USA's analytikere eller eksperter, der er udpeget til formålet, vil kunne få direkte adgang.

Det vil her være muligt at lagre data på den udpegede udbyders server for en given periode og foretage søgninger direkte på denne server. Eftersom den i TFTP-aftalen udpegede udbyder imidlertid har truffet strenge databeskyttelses- og sikkerhedsforanstaltninger, som ikke tillader identificering af de personer, der nævnes i meddelelsesdataene, er det ikke muligt at foretage

søgninger baseret på personoplysninger i den nuværende database. Der vil derfor være behov for at oprette en separat database.

Alternativt vil der kunne udtrækkes og lagres data på et andet sikkert sted i EU. USA's analytikere og eksperter, der er autoriseret til at foretage søgninger, vil enten kunne være fysisk placeret hos den udpegede udbyder eller have fjernadgang til disse data. Under alle omstændigheder og uanset hvor dataene befinder sig, vil der være behov for omfattende og solide sikringsforanstaltninger, som er skræddersyet til netop dette system.

2.3.2. Et tilsvarende EU-system

En række løsninger for et tilsvarende EU-system, som blev fremhævet i 2011-meddelelsen, er blevet vurderet, herunder et fuldstændigt centraliseret system på EU-niveau, et decentraliseret system i medlemsstaterne og tre hybridsystemer, hvor både EU og medlemsstaterne spiller en rolle.

For hver løsning er der forskellige muligheder hvad angår EU-systemets anvendelsesområde. Der skal træffes valg med hensyn til hvilke typer af meddelelser og udpegede udbydere, der skal inkluderes. Et tilsvarende EU-system kan enten holde sig til den type finansielle meddelelser og de udpegede udbydere, som p.t. er en del af TFTP-aftalen mellem EU og USA, eller bevæge sig udover disse.

- Løsningen med et fuldstændigt centraliseret system på EU-niveau vil betyde, at et enkelt EU-organ varetager alle systemets nøglefunktioner: anmodning om udtrækning af data, lagring af data, søgninger, efterretningsanalyse, sikring og overvågning af systemet og videreformidling af efterretningsoplysninger til medlemsstaterne. Denne løsning er ikke juridisk forsvarlig, da den ikke vil være i overensstemmelse med artikel 72 i TEUF, som bekræfter, at det primære ansvar for opretholdelse af lov og orden og beskyttelse af den indre sikkerhed er medlemsstaternes. Et sådant system vil hverken kunne lade sig gøre eller blive accepteret af medlemsstaterne, eftersom det ville kræve oprettelse af en form for centraliseret efterretningskapacitet på EU-niveau.
- Et fuldstændigt decentraliseret system i medlemsstaterne indebærer, at systemet forvaltes af medlemsstaternes kompetente myndigheder uden udførelse af funktioner på EU-niveau. Det ville betyde, at data kan overføres til og søges af alle

28 medlemsstater parallelt. Løsningen vil øge datastrømmene og medføre betydelige omkostninger. Det vil ligeledes føre til en øget risiko for inkonsekvent databehandling og indførelse af forskellige databeskyttelsesmekanismer. Derfor anses denne løsning ikke for brugbar.

Dermed er to løsninger udelukket fra en mere grundig gennemgang.

De tre resterende løsninger for et tilsvarende EU-system indebærer, at diverse funktioner fordeles mellem forskellige organisationer på EU-plan og nationalt plan ("hybridsystemer").

I alle disse hybridsystemer vil der løbende skulle anmodes om data fra de(n) udpegede udbyder(e), og dataene vil skulle udtrækkes og lagres i en database et sikkert sted i EU. De faktiske søgninger vil skulle foretages i denne database. Det gælder for alle løsninger, at der vil skulle træffes passende databeskyttelsesforanstaltninger.

- A) Det første hybridsystem, koordinationstjenesten og den analytiske tjeneste under EU-TFTS, indebærer oprettelse af en central TFTS-enhed på EU-plan. Enheden vil få til opgave at anmode om data fra de(n) udpegede udbyder(e), foretage søgninger, analysere efterretninger og videreformidle resultaterne. Det adskiller sig fuldstændigt fra et centraliseret system derved, at medlemsstaterne har direkte adgang til systemet og er i stand til at anmode om at få foretaget søgninger på deres vegne af en central enhed eller deres egne analytikere.

- B) Det andet hybridsystem, EU's TFTS-tjeneste for udtræk af data, vil ligeledes indebære oprettelse af en central enhed på EU-niveau. EU-organet vil dog her foretage søgninger på medlemsstaternes foranledning og videreformidle resultaterne til medlemsstaterne uden at analysere efterretningsoplysningerne. EU-organet vil have mulighed for at foretage egne søgninger og analysere resultaterne heraf.

- C) I det sidste hybridsystem, koordinationstjenesten under den finansielle efterretningsenhed[8] (FIU), vil der blive etableret en ad hoc EU-platform. Der vil ikke være tale om et permanent organ men snarere om en gruppe af eksperter i finansiel efterretning, som deltager i møder. FIU-platformen vil muligvis kunne opgraderes til dette formål. Hver enkelt medlemsstat vil kunne udpege en repræsentant, der kan

[8] Rådets afgørelse af 17. oktober 2000 om samarbejdsordninger mellem medlemsstaternes finansielle efterretningsenheder for så vidt angår udveksling af oplysninger.

handle på dens vegne. Ad hoc-myndigheden vil samle anmodninger fra hver medlemsstats FIU og på grundlag heraf anmode de(n) udpegede udbyder(e) om de pågældende data. Hver medlemsstats repræsentant vil være ansvarlig for at foretage søgninger og analysere og forvalte resultaterne på vegne af sin egen medlemsstat. Det vil herefter være op til medlemsstaternes kompetente myndigheder at gøre brug af disse efterretningsoplysninger og videreformidle dem på nationalt niveau.

2.3.3. Status quo: TFTP-aftalen mellem EU og USA

For øjeblikket kan EU og medlemsstaterne anmode USA om at foretage søgninger under TFTP-aftalen mellem EU og USA, der indeholder regler om behandling og overførsel af oplysninger om finansielle transaktioner fra den Europæiske Union til De Forenede Stater i forbindelse med programmet til sporing af finansiering af terrorisme (TFTP).

TFTP er et terrorbekæmpelsesredskab udviklet af USA i kølvandet på terroristangrebene den 11. september. Det er baseret på søgninger i de data, som den udpegede udbyder stiller til rådighed, heriblandt data fra EU.

Når de amerikanske myndigheder anmoder om data, indeholder TFTP-aftalen mellem EU og USA detaljerede regler om processen. Europol påser, at USA's anmodninger om data er i overensstemmelse med aftalen, og navnlig at de er så indsnævrede som muligt for at minimere den datamængde, der overføres. Adskillige bestemmelser omhandler sikker håndtering, lagring og sletning af dataene. Dataene opbevares i et sikkert fysisk miljø og adskilt fra andre data. Aftalen foreskriver en lagringsperiode på fem år og en forpligtelse til jævnligt at vurdere behovet for at lagre dataene. De uafhængige overvågere i USA tæller to overvågere, der er udpeget af EU. De udfører løbende kontrol med måden, systemet drives på, og har mulighed for at kontrollere enhver søgning foretaget af det amerikanske finansministerium med henblik på at sikre, at emnet for søgningen har forbindelse til terrorisme eller finansiering heraf.

Aftalen omfatter også bestemmelser om rettigheder vedrørende adgang til og berigtigelse af personoplysninger og klageprocedurer. Det fremgår af aftalen, at enhver, der mener, at hans eller hendes personoplysninger er blevet behandlet i strid med aftalen, har adgang til effektiv administrativ klage eller domstolsprøvelse i medfør af henholdsvis Den Europæiske Unions, dens medlemsstaters og USA's lovgivning. I aftalen er det endvidere fastsat, at alle personer

uanset nationalitet eller opholdsland i medfør af amerikansk lovgivning har adgang til domstolsprøvelse af bebyrdende forvaltningsakter.

De relevante forskrifter vedrørende domstolsprøvelse af bebyrdende forvaltningsakter truffet af finansministeriet i forbindelse med de personoplysninger, der er indhentet i henhold til aftalen, omfatter "Administrative Procedure Act" og "Freedom of Information act". I henhold til "Administrative Procedure Act" kan personer, der har lidt skade som følge af den amerikanske regerings embedsførelse, indbringe spørgsmålet for domstolen. I henhold til "Freedom of Information Act" kan personer anvende administrative og retlige midler til at få adgang til offentlige arkiver. De eksisterende ensrettede procedurer for adgang til og/eller berigtigelse, sletning eller blokering af personoplysninger, som Kommissionen, USA og Artikel 29-Gruppen har aftalt, har til formål at lette EU-borgernes udøvelse af disse rettigheder. Gennemførelsen af aftalen, dens sikkerhedsforanstaltninger og kontroller bliver revideret regelmæssigt i henhold til aftalens artikel 13. To sådanne revisioner blev udført i 2011[9] og 2012[10] med den konklusion, at aftalen var gennemført korrekt. Der er planlagt en tredje revision i foråret 2014. Den fælles rapport om værdien af data, som er udarbejdet i henhold til aftalens artikel 6, fremhæver fordelene ved TFTP med hensyn til forebyggelse og bekæmpelse af terror og finansiering heraf samt flere medlemsstaters anvendelse af TFTP. TFTP-oplysningerne og deres nøjagtighed gør det muligt at identificere og spore terrorister og deres støttenet overalt i verden. De kaster lys over terrororganisationers eksisterende finansielle strukturer og muliggør identificering af nye strømme af finansiel støtte og involverede parter.

3. VURDERING

Kommissionen skal i sin vurdering af, hvorvidt den agter at foreslå oprettelse af EU-TFTS, forene forskellige synspunkter og forventninger med hensyn til ambitionsniveauet for et EU-system. De enkelte interessenter og beslutningstagere ser forskelligt på målene for EU-TFTS. Kommissionen har gennemgået løsningerne og konsekvenserne ved begge scenarier ud fra de principper for udvikling og gennemførelse af førnævnte nye politiske initiativer. Hver løsning er navnlig blevet vurderet ud fra nødvendighed, proportionalitet og omkostningseffektivitet.

[9] SEK(2011) 438 af 30. marts 2011.
[10] SWD(2012) 454 af 14. december 2012.

3.1. En ramme for udtrækning af data på EU's område

Som beskrevet under punkt 2.3.1 vil løsningen med et lagrings- og udtrækningssystem være en måde, hvorpå der på EU's område kan samles, lagres og foretages søgninger i de data, der for øjeblikket overføres til USA i overensstemmelse med TFTP-aftalen mellem EU og USA. De vil altså ikke medføre yderligere efterretningsfordele for EU eller medlemsstaterne sammenlignet med den nuværende situation. Hvis TFTP-dataene derimod bliver lagret i USA og EU, vil søgninger, der p.t. foregår i ét sæt TFTP-data, blive fragmenteret og kunne have negative konsekvenser for kvaliteten og antallet af efterretningsoplysningerne og forringe TFTP's generelle effektivitet. Det vil ligeledes kunne sinke analyseprocessen, eftersom flere på hinanden følgende søgninger i TFTP-data, der lagres to forskellige steder, kan blive nødvendigt for at følge et efterretningsspor. I terrorefterforskninger er tidsfaktoren ofte afgørende.

Udtrækning af data på europæisk område fremfor i USA vil i sig selv ikke sikre en bedre beskyttelse af personoplysninger. Beskyttelse af adgang til data er afgørende for at sikre korrekt behandling af data, uanset hvor disse befinder sig. Til det formål er der behov for at træffe solide forholdsregler, som garanterer, at databehandlingen sker i overenstemmelse med de nødvendige krav. Systemet vil skulle indeholde en kontrolfunktion, som sørger for at efterprøve anmodninger om søgninger og deres begrundelser. De uafhængige overvågeres rolle vil være afgørende for at sikre, at dataene anvendes til de begrænsede formål, der er fastsat i enhver form for etableringsaftale. Der vil skulle træffes foranstaltninger for at forhindre uautoriseret adgang til eller spredning af dataene, ved f.eks. at opbevare dem i et sikkert fysisk miljø. Procedurer for adgang til og berigtigelse af personoplysninger og relevante klageprocedurer vil skulle inkorporeres. En ekstern revision vil skulle udføres for at sikre, at systemet fungerer korrekt.

Ifølge TFTP-aftalen mellem EU og USA har USA ikke adgang til alle data fra den udpegede udbyder men kun til de datasæt, som USA anmodede om, og som Europol har godkendt på grundlag af tidligere og nuværende analyser af risikoen for terrorisme. Medmindre der indføres en lignende mekanisme, hvor anmodningerne om data indsnævres fra starten, vil tilladelsen til at foretage direkte søgninger i alle data fra den udpegede udbyder medføre en øget eksponering af dataene og større konsekvenser for databeskyttelsesrettighederne. Dette vil kræve en betydelig omstrukturering af, hvordan den udpegede udbyder arbejder, og

hvordan dataene opbevares. I øjeblikket opbevares de finansielle meddelelser, som er genstand for aftalen, i en form, der ikke muliggør identifikation af de personer, der er nævnt i meddelelsesdataene. Alle finansielle meddelelser er krypterede og er kun søgbare i metadataene, dvs. datoen, hvor meddelelsen blev sendt, meddelelsestype samt de berørte afsender- og modtagerbanker. Den udpegede udbyder har truffet strenge databeskyttelses- og sikkerhedsforanstaltninger for at beskytte data fra sine kunder over hele verden. For at kunne foretage direkte søgninger på den udpegede udbyders eksisterende server vil alle disse meddelelser først skulle dekrypteres. Dette ville være overdrevet og ude af proportioner, eftersom den udpegede udbyders server indeholder flere meddelelser end dem, der er nødvendige for at bekæmpe finansiering af terror. Derudover vil direkte adgang til søgninger være hindrende og forstyrrende for den udpegede udbyders daglige virke og skabe betydelige operationelle, sikkerhedsmæssige og systemiske risici. Det vil derfor kræve, at der oprettes en separat database på EU's område, hvor de nødvendige data fra den udpegede udbyder kan opbevares.

Der vil kræve væsentlige investeringer at etablere systemet og garantere, at det overholder sikkerhedsforanstaltningerne fuldt ud. Den udpegede udbyders lokaler eller et andet sikkert sted vil skulle tilpasses de særlige krav, ligesom it-mæssige og tekniske løsninger vil skulle udvikles og vedligeholdes. Derudover vil der skulle ansættes og uddannes velkvalificeret personale, som kan forvalte og overvåge systemet.

Hvad angår denne løsning er det EU og medlemsstaterne, der skal have ulejligheden og afholde omkostningerne ved en mekanisme, der udelukkende etableres til gavn for TFTP; et instrument, der ejes af et tredjeland. Løsningen ser p.t. ud til ikke at være nødvendig, proportionel eller omkostningseffektiv, eftersom den ikke vil medføre efterretningsfordele, vil være dyr og krævende at etablere og medføre risici for beskyttelsen af personoplysninger.

3.2. Et tilsvarende EU-system

Et fuldstændigt centraliseret EU-TFTS blev udelukket fra en detaljeret vurdering, da der ikke var juridisk grundlag herfor, og det samtidig ikke var sandsynligt, at medlemsstaterne ville acceptere, at EU skulle spille en central rolle på et område, der falder ind under medlemsstaternes kompetence. Et fuldstændigt decentraliseret system blev udelukket, fordi det ville blive meget dyrt og få store konsekvenser for databeskyttelsesrettighederne. De tre

hybridsystemer, som blev vurderet, vil give medlemsstaterne en varierende grad af kontrol med de søgninger, de selv og det centraliserede EU-organ foretager.

Udvidelse af anvendelsesområdet af et tilsvarende EU-system til at dække Automated Clearance House, e-penge og andre ikke-finansielle data vil give efterretningsfordele ved at øge EU's evne til at spore betalinger inden for EU og skabe et mere fremtidssikret system end det, der blot håndterer finansielle meddelelser. Imidlertid vil enhver tilføjelse af nye udpegede udbydere øge risikoen for, at databeskyttelsesreglerne bliver brudt, og vil derfor kræve strenge betingelser og sikkerheds- og kontrolforanstaltninger. Dette vil også øge den administrative byrde, der hviler på de udpegede udbydere. Hvis der tilføjes flere dataudbydere og -meddelelser for at oprette et sådant komplekst og organisatorisk og teknisk krævende system, vil det også øge omkostningerne markant.

Som en konsekvens af denne analyse vil ethvert EU-TFTS udelukkende anvende finansielle meddelelsesdata, da Kommissionen er af den opfattelse, at de ekstra fordele ved anvendelse af flere datatyper og -udbydere ikke opvejer de betydelige omkostninger for private virksomheder og krænkelsen af retten til privatlivs- og databeskyttelse, som et sådant system vil medføre. Eftersom EU-systemet kun vil dække den samme udpegede udbyder og samme meddelelsestype som TFTP, vil kvaliteten og kvantiteten af de modtagede efterretninger såvel som de eksponerede data være sammenlignelige med TFTP-aftalen mellem EU og USA.

Som nævnt ovenfor er der tre løsninger for udforming af et tilsvarende EU-system: A) Koordinationstjenesten og den analytiske tjeneste under EU-TFTS, B) EU's TFTS-tjeneste for udtræk af data og C) Koordinationstjenesten under den finansielle efterretningsenhed (FIU).

Løsning A) vil sandsynligvis have en positiv indflydelse hvad angår forebyggelse af terrorisme og øget sikkerhed i EU. Hvis grupper i både EU og medlemsstaterne foretager søgninger og analyserer resultater, vil det i nogen grad sikre, at EU og medlemsstaternes specifikke efterretningskrav bliver opfyldt fuldt ud, og at systemet er indrettet efter den specifikke trussel mod EU. Denne forbedring er imidlertid betinget af, at medlemsstaterne på mellemlang til lang sigt viser sig mere villige og i stand til at dele oplysninger og analyser. Det er uklart, i hvilket omfang denne øgede informationsstrøm er pålidelig. Dertil kommer, at selvom medlemsstaten fortsat kan anmode USA om søgninger i henhold til TFTP-aftalen, vil

dette system kræve betydelige investeringer og samarbejde fra medlemsstaternes side, hvis det skal kunne give et mere sammenhængende EU-billede.

Løsning B) vil kunne have en vis positiv indflydelse hvad angår forebyggelse af terrorisme og øget sikkerhed i EU. Systemet vil i højere grad kunne bidrage til EU's trusselsanalyser, da søgningerne vil blive foretaget i overensstemmelse med medlemsstaternes specifikke efterretningskrav. Et centraliseret EU-organ ville imidlertid være begrænset til at foretage søgninger og videreformidle de tilhørende data til den medlemsstat, der anmoder herom. Det ville altså først og fremmest fungere som en form for adgangskontrol. Der vil følgelig ikke blive foretaget analyser på EU-niveau, og systemet vil være fuldstændig afhængigt af, at medlemsstaterne deler analyserne indbyrdes uden for systemet, hvis der skal tegnes et sammenhængende EU-efterretningsbillede. Systemets manglende evne til at garantere en ensartet tilgang til søgningernes udformning vil øge risikoen for falsk positive resultater og dermed få konsekvenser for databeskyttelse og retten til privatlivets fred.

Løsning C) vil dække medlemsstaternes specifikke efterretningsbehov og således have en vis positiv virkning hvad angår forebyggelse af terrorisme og øget sikkerhed. Eftersom nationale FIU'er vil være ansvarlige for søgninger og analyser for deres medlemsstater, har denne løsning samme ulemper som løsning B), hvor der kun kan tegnes et klart billede via medlemsstaternes øgede samarbejde uden for systemet. Derudover vil FIU's eksklusive fokus på finansiel efterretning og kløften mellem disse oplysninger og den bredere efterretning gøre det mere vanskeligt at se forbindelser og spore finansiering af terror. Der er også en meget lille grad af EU-engagement i denne løsning, og kapaciteten vil primært blive øget på nationalt niveau.

Alle løsninger vil medføre betydelige omkostninger for EU, medlemsstaterne og de udpegede udbydere, herunder bl.a. omkostninger til udvikling af it-infrastrukturen, sikkerhedsfaciliteter og omkostninger i forbindelse med de formentlig flere hundrede ansatte, der skal forvalte systemet og gennemføre sikkerheds- og kontrolforanstaltningerne. Hvert af de mulige systemer vil dog potentielt kunne bidrage til en forbedret sikkerhedssituation i Europa, idet de anvendte trusselsvurderinger vil være målrettet europæiske behov.

Et uafhængigt efterretnings- og efterforskningsværktøj på europæisk område vil fjerne kravet om overførelse af data til USA. Et EU-TFTS vil dog stadig kræve omfattende

databeskyttelsesforanstaltninger, der ligner dem, som allerede anvendes inden for rammerne af TFTP-aftalen mellem EU og USA, og som under alle omstændigheder overholder EU og medlemsstaternes databeskyttelsesregler. Enhver anmodning om søgninger i data i EU's systemer vil skulle kontrolleres for, om den overholder de strenge formålsbegrænsninger for bekæmpelse af terrorisme og finansiering heraf, herunder om overførslen af data er berettiget. Det vil især kræve kvalificerede uafhængige overvågere, der skal efterprøve, at alle EU og medlemsstaternes søgninger er behørigt godkendt og nødvendige for at bekæmpe terrorisme og finansiering heraf. Der skal sørges for sikker håndtering og lagring af data, og uautoriseret adgang til dataene skal forhindres. Det vil være nødvendigt at foretage en ekstern revision af, at systemet og alle dets sikkerhedsforanstaltninger er velfungerende. Alle nødvendige procedurer for adgang til og berigtigelse af personoplysninger og relevante klageprocedurer vil skulle integreres i systemet.

Konkluderende har Kommissionen i overensstemmelse med Europa-Parlamentets og Rådets anmodninger vurderet de mulige løsninger for et EU-TFTS, heriblandt et lagrings- og udtrækningssystem.

Denne vurdering tager højde for principperne i den informationsstyringsstrategi, der blev vedtaget under det svenske EU-formandsskab. Ethvert system, der etableres, skal være nødvendigt, proportionelt og omkostningseffektivt og respektere grundlæggende rettigheder. Kommissionens analyse, der fremgår af ovenstående og af konsekvensanalysen, viser, at alle de mulige løsninger har fordele og ulemper. Kommissionen har dog valgt at se bort fra de løsninger, der ikke kan realiseres, hvilket der også er redegjort for i ovenstående.

Set i lyset af de indhentede oplysninger, er det på nuværende tidspunkt ikke oplagt at fremlægge et forslag til et EU-TFTS.

Kommissionen hører gerne, om Europa-Parlamentet og Rådet har bemærkninger til denne meddelelse.