

Bryssel den 27.11.2013
COM(2013) 842 final

**MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH
RÅDET**

Ett europeiskt system för att spåra finansiering av terrorism (EU TFTS)

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

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Ett europeiskt system för att spåra finansiering av terrorism (EU TFTS)

Detta meddelande är en uppföljning av meddelandet av den 13 juli 2011 (KOM(2011) 429) och syftar till att informera Europaparlamentet och rådet om resultaten av de analyser som gjorts med avseende på genomförbarheten av ett europeiskt system för att spåra finansiering av terrorism (nedan även kallat *EU TFTS* eller *EU-system*).

1. BAKGRUND

1.1. Bakgrund och definitioner

Under förhandlingarna inför ingåendet av TFTP-avtalet mellan EU och Förenta staterna¹ fördes diskussioner om hur man bäst kan skydda personuppgifter och respektera de grundläggande rättigheterna inom ramen för avtalet. Vissa parter framhöll att om uppgifter framtas på EU:s territorium skulle detta begränsa den mängd data som överförs till Förenta staterna, och därför skulle detta alternativ utgöra en bättre garanti för uppgiftsskyddet. Några medlemsstater såg ett mervärde i att på längre sikt utveckla ett oberoende europeiskt system för att spåra finansiering av terrorism. Europaparlamentet uppmanade rådet och kommissionen att vidta alla nödvändiga åtgärder för att ta fram en varaktig och rättsligt korrekt europeisk lösning på problemet med framtagning av begärda uppgifter på europeiskt territorium. Rådet och Europaparlamentet uppmanade i samband med godkännandet av TFTP-avtalet kommissionen att inom ett år från dagen för avtalets ikraftträdande överlämna en rättslig och teknisk ram för framtagning av information på EU:s territorium och att senast tre år från dagen för avtalets ikraftträdande lägga fram en rapport om framstegen i fråga om utvecklingen av ett motsvarande EU-system². Dessutom anges det i artikel 11 i TFTP-avtalet att kommissionen under avtalets löptid kommer att genomföra en undersökning rörande möjligheterna att införa ett motsvarande EU-system som möjliggör en mer riktad överföring av uppgifter.

För detta meddelandes syften bör åtskillnad göras mellan ”ett motsvarande EU-system” och ”en ram för framtagning av information på EU:s territorium”. *En ram för framtagning av*

¹ EUT L 195, 27.7.2010, s. 5.

² Rådets beslut av den 13 juli 2010, EUT L 195, 27.7.2010, s. 3.

information på EU:s territorium ska förstås som ett system som gör det möjligt att på EU:s territorium genomföra sökningar i uppgifter som EU för närvarande lämnar till Förenta staterna. *Ett motsvarande EU-system* skulle däremot vara ett oberoende europeiskt system för att spåra finansiering av terrorism genom åtkomst till, sökningar i och analys av den eller de utsedda tillhandahållarnas uppgifter. Oavsett vilket EU-system som inrättas skulle det kräva ändringar av TFTP-avtalet mellan EU och Förenta staterna.

1.2. Vidtagna åtgärder

I december 2010 lät kommissionen genomföra en undersökning som i juli 2011 utsträcktes till att omfatta ytterligare ett alternativ, ett system för lagring och framtagning. Under undersökningens gång höll kommissionen fyra expertmöten med berörda parter, bl.a. Europol, Europeiska datatillsynsmannen, den utsedda tillhandahållaren enligt TFTP-avtalet³ och många experter från medlemsstaterna som företrädde berörda ministerier, brottsbekämpande organ, underrättelsetjänster och dataskyddsmyndigheter.

Kommissionen lade i sitt *meddelande till Europaparlamentet och rådet* av den 13 juli 2011 (nedan kallat *meddelandet från 2011*) fram fem möjliga alternativ som kommissionen hade identifierat för ett EU-system för att spåra finansiering av terrorism. Av dessa ansågs tre vara genomförbara. Syftet med 2011 års meddelande var att inleda en debatt om vägen framåt och ge input till den konsekvensbedömning som skulle göras.

I oktober 2011 togs frågan upp i rådet (rättsliga och inrikes frågor) och Europaparlamentets utskott för medborgerliga fri- och rättigheter.

Eftersom medlemsstaterna och Europaparlamentet inte uttryckte en tydlig preferens för något av alternativen beslutades det att alla skulle omfattas av kommissionens konsekvensbedömning och att de skulle vidareutvecklas genom att olika delalternativ togs fram. Detta meddelande bygger på konsekvensbedömningen⁴.

³ Society for Worldwide Interbank Financial Telecommunication (SWIFT).

⁴ SWD(2013) xx av den

2. KOMMISSIONENS CENTRALA PRINCIPER OCH FASTSTÄLLDA ALTERNATIV

2.1. Principer för den informationshanteringsstrategi som antogs under det svenska ordförandeskapet

I sin analys av den föreslagna vägen framåt tar kommissionen hänsyn till de grundläggande principer som fastställdes i 2009 års informationshanteringsstrategi⁵ och som senare införlivats och vidareutvecklats i kommissionens meddelanden från 2010 om översikt av informationshanteringen inom området med frihet, säkerhet och rättvisa⁶ och från 2012 om den europeiska modellen för informationsutbyte⁷.

Avgörande i detta avseende är principerna om att skydda grundläggande rättigheter, nödvändighet, proportionalitet och kostnadseffektivitet.

Att skydda de *grundläggande rättigheter* som fastställs i Europeiska unionens stadga om de grundläggande rättigheterna, särskilt rätten till personlig integritet och skydd av personuppgifter, är en prioriterad fråga för kommissionen vid utarbetandet av nya förslag som rör behandling av personuppgifter på området inre säkerhet. I artiklarna 7 och 8 i stadgan uttrycks vars och ens rätt till ”respekt för sitt privatliv och familjeliv” och ”skydd av de personuppgifter som rör honom eller henne”. I artikel 16 i fördraget om Europeiska unionens funktionssätt (nedan kallat *EUF-fördraget*), som är bindande för medlemsstaterna och unionens institutioner, byråer och organ, bekräftas vars och ens rätt till ”skydd av de personuppgifter som rör honom eller henne”. Enligt artikel 52 i stadgan får begränsningar i utövandet av de rättigheter och friheter som erkänns i stadgan, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

Intrång i rätten till personlig integritet anses *nödvändigt* om det är ett svar på ett trängande behov, om det står i proportion till det syfte som ska uppnås och om de skäl som läggs fram av den offentliga myndigheten är relevanta och tillräckliga.

⁵ Rådets slutsatser av den 30 november 2009 om en informationshanteringsstrategi för EU:s inre säkerhet, 16637/09.

⁶ KOM(2010) 385 av den 20 juli 2010.

⁷ COM(2012) 735 av den 7 december 2012.

Även om det är svårt att bedöma alla kostnader som terrorism ger upphov till i ekonomiska termer, kvarstår principen om *kostnadseffektivitet*. En *kostnadseffektiv* metod väger in befintliga lösningar för att minimera överlappning och maximera möjliga synergier. En bedömning krävs av huruvida det är möjligt att nå målen med ett förslag genom en effektivare användning av befintliga instrument.

2.2. Tillvägagångssätt

Mot bakgrund av de principer som avses ovan har kommissionen undersökt huruvida ett EU-system för att spåra finansiering av terrorism skulle vara nödvändigt och proportionellt med avseende på kostnaderna, fördelarna samt konsekvenserna för de grundläggande rättigheterna, jämfört med den nuvarande situationen.

När det gäller *fördelar* skulle ett EU-system kunna öka EU:s och medlemsstaternas kapacitet att få åtkomst till relevanta uppgifter och stärka deras analytiska kapacitet att spåra och identifiera terrorister genom finansiella transaktioner. Eftersom finansiella transaktioner kan ge värdefulla underrättelser som kanske inte kan fås från andra källor skulle detta verktyg ha ett särskilt värde när det gäller att upptäcka terroristverksamhet och inblandade aktörer. Därför skulle ett EU-system kunna utgöra ytterligare ett underrättelse- och utredningsverktyg i kampen mot terrorism och i arbetet med att förbättra säkerheten inom EU, särskilt om ett sådant system skulle omfatta ett flertal tillhandahållare av finansiella uppgifter och ett flertal typer av transaktioner. Fördelarna med ett EU-system måste vägas mot de beräknade kostnaderna för införande och upprätthållande av ett sådant system, inklusive den ekonomiska bördan för EU, medlemsstaterna och de utsedda tillhandahållarna av de berörda uppgifterna.

2.3. Presentation av alternativen

Ett antal alternativ både för *ramen för framtagning av information på EU:s territorium* och för *ett motsvarande EU-system* har övervägts.

2.3.1. En ram för framtagning av uppgifter på EU:s territorium

En ram för framtagning av uppgifter på EU:s territorium skulle kunna genomföras genom ett system för lagring och framtagning av uppgifter som innehas av den utsedda tillhandahållaren, genom att direkt åtkomst ges till de uppgifter som för närvarande lämnas till Förenta staterna inom ramen för TFTP-avtalet. Denna direkta åtkomst skulle ges till amerikanska analytiker eller experter som bemyndigats för detta ändamål.

Inom ramen för detta alternativ skulle en möjlighet vara att lagra uppgifter på en server hos den utsedda tillhandahållaren under en bestämd tid och göra sökningar direkt på servern. Den nuvarande utsedda tillhandahållaren enligt TFTP-avtalet mellan EU och Förenta staterna har emellertid infört strikta uppgiftsskydds- och säkerhetsåtgärder som inte medger identifiering av personer som nämns i meddelandens datainnehåll, varför det inte går att göra sökningar utifrån personuppgifter i dess nuvarande databas. Därför skulle man behöva skapa en separat databas.

Alternativt skulle uppgifter kunna framtas och lagras på en annan säker plats i EU. Amerikanska analytiker eller experter som bemyndigats att genomföra sökningar skulle antingen kunna finnas fysiskt på plats hos den utsedda tillhandahållaren eller ha fjärråtkomst till uppgifterna. I samtliga fall, och oavsett var uppgifterna befinner sig, skulle omfattande och tillförlitliga skyddsåtgärder behöva införas och anpassas till systemets utformning.

2.3.2. Ett motsvarande EU-system

Ett antal alternativ för ett motsvarande EU-system (som det beskrivs i meddelandet från 2011) har bedömts, inklusive ett helt centraliserat system på EU-nivå, ett decentraliserat system på medlemsstatsnivå och tre hybridsystem där både EU och medlemsstaterna skulle spela en roll.

Varje alternativ ger olika möjligheter när det gäller EU-systemets omfattning. Det måste också beslutas vilka typer av meddelanden och utsedda tillhandahållare som skulle ingå. Ett motsvarande EU-system skulle kunna avse samma typ av finansiella meddelanden och utsedda tillhandahållare som för närvarande omfattas av TFTP-avtalet, eller gå längre.

- Alternativet med ett helt centraliserat system på EU-nivå skulle innebära att ett enda EU-organ skulle utföra alla huvudfunktionerna inom systemet: begära framtagning av uppgifter, lagra uppgifter, göra sökningar, göra underrättelseanalyser, skydda och övervaka systemet och sprida underrättelser till medlemsstaterna. Detta alternativ är emellertid rättsligt osunt eftersom det inte skulle följa artikel 72 i EUF-fördraget, där det bekräftas att det primära ansvaret för att upprätthålla lag och ordning och skydda den inre säkerheten ligger hos medlemsstaterna. Ett sådant system skulle varken vara genomförbart eller godtagbart för medlemsstaterna, eftersom det skulle vara nödvändigt att inrätta någon form av centraliserad underrättelsekapacitet på EU-nivå.

- Ett helt decentraliserat system på medlemsstatsnivå skulle innebära att systemet skulle skötas av medlemsstaternas behöriga myndigheter och att inga funktioner skulle utföras på EU-nivå. Detta innebär att uppgifter skulle kunna överföras till och sökningar göras av alla 28 medlemsstaterna parallellt. Detta alternativ skulle leda till mångdubbelt fler dataflöden och betydande kostnader. Det skulle också medföra en ökad risk för att uppgifter behandlas inkonsekvent och att oenhetliga uppgiftsskyddsmekanismer införs. Detta alternativ betraktas därför inte heller som genomförbart.

Dessa två alternativ har därför inte tagits med i den mer utförliga bedömningen.

De tre övriga alternativen för ett motsvarande EU-system (nedan kallade *hybridsystem*) innebär att de olika funktionerna fördelas mellan olika organisationer på EU-nivå och nationell nivå.

I alla dessa hybridsystem skulle uppgifter begäras löpande och iterativt från den eller de utsedda tillhandahållarna, framtas samt lagras i en databas på en säker plats i EU. De faktiska sökningarna skulle sedan göras mot denna centrala databas. På samma sätt för alla alternativ skulle lämpliga uppgiftsskyddsgarantier behöva inrättas.

- A) I det första hybridsystemet, en samordnings- och analystjänst för EU TFTS, skulle en central EU-enhet behöva skapas. Den skulle få i uppdrag att begära uppgifter från den eller de utsedda tillhandahållarna, göra sökningar, analysera underrättelser och sprida resultaten. Skillnaden jämfört med ett helt centraliserat system skulle vara att medlemsstaterna skulle få direkt åtkomst till systemet och skulle kunna begära att sökningar görs för deras räkning av den centrala enheten eller av deras egna analytiker.
- B) Det andra hybridsystemet, en dataframtagningstjänst för EU TFTS, skulle också innebära att det skapas en central EU-enhet. Enligt detta alternativ skulle EU-enheten göra sökningar på begäran av medlemsstaterna men sprida resultaten till medlemsstaterna utan att analysera underrättelserna. EU-enheten skulle dock kunna göra egna sökningar och analysera resultatet av dem.

- C) I det tredje hybridsystemet, en samordningstjänst för finansunderrättelseenheter⁸, skulle en särskild EU-plattform skapas. Denna tjänst skulle inte vara ett permanent organ, utan en grupp av finansunderrättelseexperter som deltar i möten. Den befintliga plattformen för finansunderrättelseenheter (FIU-plattformen) skulle möjligen kunna uppgraderas för detta ändamål. Varje medlemsstat skulle utse en företrädare som skulle agera på dess vägnar. Denna tillfälliga myndighet skulle sammanställa förfrågningar om uppgifter från varje medlemsstats finansunderrättelseenheter och begära uppgifter från den eller de utsedda tillhandahållarna på grundval av dessa förfrågningar från medlemsstaterna. Varje medlemsstats företrädare skulle ansvara för att göra sökningar, utföra analyser och förvalta resultaten på den egna medlemsstatens vägnar. Det skulle sedan ankomma på medlemsstaternas behöriga myndigheter att använda underrättelserna och sprida dessa uppgifter på nationell nivå.

2.3.3. *Status quo: TFTP-avtalet mellan EU och Förenta staterna*

För närvarande kan EU och medlemsstaterna begära att sökningar görs av Förenta staterna enligt avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP).

Programmet för att spåra finansiering av terrorism (nedan kallat *TFTP-programmet*) är ett redskap i kampen mot terrorism som utarbetades av Förenta staterna i efterdyningarna av terroristattacker den 11 september. Det bygger på sökningar i de uppgifter som utsedda tillhandahållare tillhandahåller, däribland uppgifter som överförs från EU.

TFTP-avtalet mellan EU och Förenta staterna reglerar i detalj processen för de amerikanska myndigheternas begäran om uppgifter. Europol kontrollerar att de begäranden om uppgifter som inkommer från Förenta staterna överensstämmer med avtalet och, i synnerhet, att de är så välavgränsade som möjligt för att minimera den mängd data som överförs. Många bestämmelser gäller för säker hantering, lagring och utplåning av uppgifter. Tillhandahållna uppgifter bevaras i en säker fysisk miljö och lagras separat från andra uppgifter. Avtalet föreskriver en lagringsperiod på fem år och en skyldighet att regelbundet utvärdera behovet av att lagra uppgifterna. De oberoende övervakarna är belägna i USA och omfattar två

⁸ Rådets beslut av den 17 oktober 2000 om en samarbetsordning för medlemsstaternas finansunderrättelseenheter avseende utbyte av information.

övervakare som EU har utsett. De utövar kontinuerlig kontroll över hur systemet fungerar och har möjlighet att kontrollera varje sökning som görs av Förenta staternas finansministerium för att säkerställa att det finns en koppling mellan den som är föremål för sökningen och terrorism eller dess finansiering.

Avtalet innehåller också bestämmelser om rätten att ta del av personuppgifter och rätten till rättelse av personuppgifter samt om förfaranden för prövning. Enligt avtalet har varje person som anser att hans eller hennes personuppgifter har behandlats på ett sätt som strider mot avtalet rätt att söka effektiv administrativ eller rättslig prövning i enlighet med lagstiftningen i Europeiska unionen, dess medlemsstater respektive Förenta staterna. Det fastställs också att var och en, oavsett nationalitet eller bosättningsland, enligt amerikansk lag ska ha tillgång till domstolsprövning av administrativa beslut som gått vederbörande emot.

Relevanta författningar som gäller för ansökan om prövning av ett administrativt beslut av finansministeriet som gått vederbörande emot och som har samband med personuppgifter som mottagits i enlighet med detta avtal är bl.a. *Administrative Procedure Act* och *Freedom of Information Act*. *Administrative Procedure Act* ger personer som har lidit skada till följd av Förenta staternas regerings åtgärder att ansöka om prövning av åtgärdens lagenlighet. *Freedom of Information Act* ger personer möjlighet att använda administrativa och rättsliga medel för att söka i offentliga register. De befintliga enhetliga förfaranden för att ta del av och/eller för rättelse, radering eller blockering av personuppgifter som överenskommit mellan kommissionen, Förenta staterna och artikel 29-arbetsgruppen syftar till att underlätta för EU-medborgare att utöva dessa rättigheter. Genomförandet av avtalet och dess skyddsåtgärder och kontroller är föremål för regelbundna översyner enligt artikel 13 i avtalet. Två sådana översyner gjordes 2011⁹ och 2012¹⁰, och slutsatsen blev att avtalet hade genomförts på ett korrekt sätt. En tredje översyn planeras våren 2014. Den gemensamma rapport om värdet av tillhandahållna uppgifter som utarbetats i enlighet med artikel 6 i avtalet visar att TFTP-uppgifter varit till nytta för att förebygga och bekämpa terrorism och dess finansiering samt att TFTP-uppgifter använts i flera medlemsstater. TFTP-uppgifter och deras exakthet gör det möjligt att identifiera och spåra terrorister och deras stödnätverk i hela

⁹ SEK(2011) 438 av den 30 mars 2011.

¹⁰ SWD(2012) 454 av den 14 december 2012.

världen. De ger en inblick i de befintliga finansiella strukturerna för terroristorganisationer och möjliggör identifiering av nya typer av finansiellt stöd och av de berörda aktörerna.

3. BEDÖMNING

Vid bedömningen av huruvida man ska föreslå inrättandet av ett EU-system för att spåra finansiering av terrorism eller ej måste kommissionen väga samman de olika synpunkterna och förväntningar när det gäller ambitionsnivån för ett EU-system. Målen för ett EU-system ses på olika sätt av olika berörda parter och beslutsfattare. Kommissionen har undersökt möjligheterna med och effekterna av båda scenarierna mot bakgrund av de principer för utarbetande och genomförande av nya politiska initiativ som beskrivs ovan. Särskilt har varje alternativ vägts i fråga om nödvändighet, proportionalitet och kostnadseffektivitet.

3.1. En ram för framtagning av uppgifter på EU:s territorium

Som beskrivs i avsnitt 2.3.1 skulle alternativet med ett system för lagring och framtagning av uppgifter utgöra ett sätt att på EU:s territorium samla in, lagra och göra sökningar i uppgifter som för närvarande överförs till Förenta staterna enligt TFTP-avtalet. Det skulle alltså inte ge upphov till ytterligare underrättelsefördelar för EU eller medlemsstaterna jämfört med den nuvarande situationen. Tvärtom skulle det faktum att TFTP-uppgifter skulle lagras både i Förenta staterna och i EU leda till en fragmentering av sökningar som för närvarande görs mot en enda uppsättning TFTP-uppgifter, vilket skulle kunna få negativa följder för kvaliteten på underrättelserna och deras antal samt inverka menligt på den övergripande effektiviteten i TFTP-programmet. Det skulle också i betydande grad kunna sakta ner analysprocessen, eftersom det kan bli nödvändigt att göra flera på varandra följande sökningar i TFTP-uppgifter som lagras på två ställen för att följa upp en underrättelse. Snabbhet är ofta avgörande när det gäller utredningar av terrorism.

Framtagning av uppgifter på EU:s territorium i stället för i Förenta staterna skulle inte i sig säkerställa ett bättre skydd av personuppgifter. För att säkerställa en korrekt hantering av uppgifter är skyddad åtkomst till uppgifterna avgörande, oavsett var de befinner sig. För detta ändamål skulle en uppsättning kraftfulla skyddsåtgärder behöva inrättas som skulle garantera att behandlingen och hanteringen av data uppfyller de nödvändiga kraven. Systemet måste vara utrustat med en kontrollfunktion som ansvarar för kontrollen av sökförfrågningar och av skälen till dem. De oberoende övervakarna skulle spela en avgörande roll när det gäller att

säkerställa att uppgifter används för de begränsade ändamål som fastställs i ett avtal om inrättande. Åtgärder behöver vidtas för att förhindra att obehöriga får tillträde till uppgifter eller att uppgifter lämnas ut, t.ex. genom att bevara uppgifterna i en säker fysisk miljö. Förfaranden för att ta del av personuppgifter och för rättelse av personuppgifter samt relevanta prövningsförfaranden skulle behöva byggas in. En extern revision måste utföras för att säkerställa att systemet fungerar korrekt.

Enligt TFTP-avtalet har Förenta staterna inte åtkomst till alla den utsedda tillhandahållarens uppgifter, utan endast till uppgifter som Förenta staterna har begärt och som har godkänts av Europol på grundval av tidigare och aktuella riskanalyser. Om en liknande mekanism för att inledningsvis avgränsa begäran om uppgifter inte införs, skulle möjligheten att göra direkta sökningar i alla den utsedda tillhandahållarens uppgifter ytterligare öka uppgifternas exponering och inverkan på rättigheter avseende uppgiftsskydd. Detta skulle kräva genomgripande ändringar av den utsedda tillhandahållarens arbetssätt och hur dess uppgifter lagras. För närvarande bevaras finansiella meddelanden som omfattas av avtalet i en form som omöjliggör identifiering av personer som anges i meddelandenas datainnehåll. Varje finansiellt meddelande krypteras och sökningar kan endast göras på metadata, dvs. den dag meddelandet sändes, typ av meddelande samt de avsändande och mottagande banker som var involverade. Den utsedda tillhandahållaren har infört strikta uppgiftsskydds- och säkerhetsåtgärder för att skydda uppgifter rörande dess kunder i hela världen. För att möjliggöra sökningar direkt på den nuvarande utsedda tillhandahållarens server skulle därför alla dessa meddelanden först behöva dekrypteras. Detta skulle bli orimligt och oproportionellt, eftersom den utsedda tillhandahållarens server innehåller andra meddelanden än de som är nödvändiga för att bekämpa finansiering av terrorism. Dessutom skulle direkt åtkomst för sökändamål inkräkta orimligt mycket på den utsedda tillhandahållarens dagliga verksamhet och skapa betydande operativa risker och säkerhets- och systemrisker. Därför skulle detta kräva att en separat databas skapas på EU:s territorium för att bevara de av den utsedda tillhandahållarens uppgifter som är nödvändiga.

Stora investeringar skulle behövas för att införa systemet och garantera att det till fullo överensstämmer med säkerhetsåtgärderna. Den utsedda tillhandahållarens lokaler eller en annan säker plats måste anpassas till de specifika kraven, it-lösningar och andra tekniska

lösningar måste utarbetas och underhållas och högt kvalificerad personal för att förvalta och övervaka systemet måste anställas och utbildas.

Detta alternativ innebär att EU och medlemsstaterna skulle bära alla olägenheter och kostnader för en mekanism som inrättas enbart för TFTP-programmet, som är ett instrument som ägs av ett tredjeland. För närvarande förefaller detta alternativ inte vara nödvändigt, proportionellt eller kostnadseffektivt, eftersom det inte skulle medföra några ytterligare underrättelseförmåner och eftersom det skulle bli kostsamt, vara krävande att inrätta och kunna skapa risker avseende skyddet av personuppgifter.

3.2. Ett motsvarande EU-system

Alternativet med ett helt centraliserat EU-system togs inte med i den mer detaljerade bedömningen på grund av avsaknaden av rättslig grund och osannolikheten för att medlemsstaterna skulle godta centralisering på EU-nivå på ett område där medlemsstaterna är behöriga. Alternativet med ett helt decentraliserat system togs inte heller med på grund av att det skulle ha medfört stora kostnader och en mångdubbelt större inverkan på rättigheter avseende uppgiftsskydd. De tre hybridsystem som bedömdes skulle i olika hög grad ge medlemsstaterna kontroll över de sökningar som görs av dem själva och av det centraliserade EU-organet.

En utvidgning av räckvidden för ett motsvarande EU-system till att omfatta automatiserade clearingorganisationer, e-pengar och andra uppgifter som inte är FIN-uppgifter skulle medföra underrättelsefördelar genom att öka EU:s förmåga att spåra betalningar inom EU och skulle kunna skapa ett mer "framtidspanpassat" system än ett som endast inriktas på FIN-meddelanden. Varje ökning av antalet utsedda tillhandahållare skulle emellertid öka risken för överträdelser av rättigheterna avseende uppgiftsskydd och skulle därför kräva en strikt uppsättning villkor, skyddsåtgärder och kontrollåtgärder. Detta skulle också öka den administrativa belastningen för de utsedda tillhandahållarna. Att skapa ett sådant komplext och organisatoriskt och tekniskt krävande system med ett flertal tillhandahållare av uppgifter och ett flertal meddelandetyper skulle också öka kostnaderna avsevärt.

Följden av denna analys är att ett genomförbart EU-system endast skulle använda FIN-meddelanden, eftersom kommissionen anser att de ytterligare fördelarna med att använda ett flertal uppgiftstyper och tillhandahållare inte uppväger de betydande kostnader för privata

företag och den skada för rätten till integritet och uppgiftsskydd som ett sådant system skulle medföra. Eftersom EU-systemet endast skulle omfatta samma utsedda tillhandahållare och samma meddelandetyp som TFTP-avtalet, skulle de mottagna underrättelsernas kvalitet och kvantitet samt uppgifternas exponering således vara jämförbar med vad som uppnås inom ramen för TFTP-avtalet mellan EU och Förenta staterna.

Såsom anges ovan finns det tre alternativ för ett motsvarande EU-system: A) en samordnings- och analystjänst för EU TFTS, B) en dataframtagningstjänst för EU TFTS och C) en samordningstjänst för finansunderrättelseenheter.

Alternativ A skulle kunna förväntas ha en positiv inverkan när det gäller att förebygga terrorism och förbättra säkerheten i EU. I och med att både EU och medlemsstaterna skulle göra sökningar och analysera resultaten skulle man bättre garantera att de specifika underrättelsekraven i EU och medlemsstaterna beaktas i deras helhet och att systemet är inriktat på specifika "EU-hot". Denna förbättring är dock beroende av att medlemsstaternas vilja och förmåga att utbyta information och analyser ökar på medellång till lång sikt. Det är oklart i vilken utsträckning man kan räkna med detta ökade informationsutbyte. Eftersom medlemsstaterna fortfarande skulle ha möjlighet att begära sökningar från Förenta staterna inom ramen för TFTP-avtalet skulle detta system dessutom behöva avsevärd uppbackning och samarbete från medlemsstaternas sida för att kunna ge en mer enhetlig europeisk bild.

Alternativ B skulle kunna ha en viss positiv inverkan när det gäller att förebygga terrorism och förbättra säkerheten i EU. Systemet skulle vara mer lyhört för EU:s hotbildsanalyser, eftersom sökningarna skulle göras på grundval av de specifika underrättelsekraven i medlemsstaterna. Det centraliserade EU-organets roll skulle dock begränsas till att göra sökningar och överföra de uppgifter som en medlemsstat har begärt. Det skulle alltså snarast fungera som en kontrollinstans. Till följd av detta skulle det inte finnas några analyser på EU-nivå, och systemet skulle vara helt beroende av att medlemsstaterna utbyter analyser med varandra utanför systemet för att en enhetlig europeisk underrättelsebild skulle kunna skapas. Systemets oförmåga att garantera ett enhetligt tillvägagångssätt för avgränsning av sökningar skulle öka risken för falskt positiva resultat och på så sätt inkräkta på rättigheterna avseende uppgiftsskydd och integritet.

Alternativ C skulle kunna anpassas till medlemsstaternas särskilda underrättelsebehov och skulle därmed ha en viss positiv inverkan på att förebygga terrorism och förbättra säkerheten. Eftersom de nationella finansunderrättelseenheterna skulle ansvara för deras respektive medlemsstaters sökningar och analyser medför detta alternativ samma nackdelar som alternativ B – en tydlig bild kan uppnås endast genom ett ökat samarbete mellan medlemsstaterna, utanför systemet. Dessutom fokuserar finansunderrättelseenheterna endast på finansunderrättelser, och avståndet mellan denna information och den bredare underrättelsemiljön skulle kunna göra det svårare att se samband och upptäcka finansiering av terrorism. Graden av EU:s deltagande i detta alternativ är mycket låg, och kapaciteten skulle förbättras främst på nationell nivå.

Alla dessa alternativ skulle medföra stora kostnader för EU, medlemsstaterna och den utsedda tillhandahållaren, däribland kostnaden för utveckling av it-infrastruktur, säkra lokaler och tiotals eller t.o.m. hundratals anställda för att förvalta systemet och genomföra säkerhetsåtgärder och kontroller. Vart och ett av dessa möjliga system har dock potential att bidra till ett bättre säkerhetsläge i Europa, eftersom de skulle använda hotbedömningar som är specifika för europeiska behov.

Ett oberoende underrättelse- och utredningsinstrument på europeiskt territorium skulle undanröja kravet på överföring av data till Förenta staterna. Men alla potentiella EU-system skulle fortfarande kräva omfattande skyddsåtgärder och kontroller som liknar dem som redan gäller inom ramen för TFTP-avtalet mellan EU och Förenta staterna och som under alla omständigheter uppfyller EU:s och medlemsstaternas regelverk i fråga om uppgiftsskydd. Varje begäran om sökningar av uppgifter i EU:s system skulle behöva genomgå en kontroll av att ändamålet är strikt begränsat till att bekämpa terrorism och dess finansiering, inklusive en kontroll av huruvida överföringen av uppgifter är befogad. I synnerhet skulle det krävas kvalificerade oberoende övervakare för att kontrollera att varje sökning som görs av EU eller en medlemsstat är vederbörligen bemyndigad och nödvändig för ändamålet att bekämpa terrorism och dess finansiering. Säker hantering och lagring av uppgifterna måste garanteras och obehörig åtkomst till uppgifterna förhindras. En extern revision av systemets och alla dess skyddsåtgärders funktion skulle vara nödvändig. Alla nödvändiga förfaranden för att ta del av personuppgifter och för rättelse av personuppgifter samt relevanta prövningsförfaranden skulle behöva införlivas i systemet.

Sammanfattningsvis har kommissionen i linje med Europaparlamentets och rådets önskemål utvärderat de möjliga alternativen för ett EU-system för att spåra finansiering av terrorism, inklusive ett system för framtagning och lagring av uppgifter.

Denna bedömning tar hänsyn till principerna i den informationshanteringsstrategi som antogs under det svenska ordförandeskapet. Ett eventuellt system måste vara nödvändigt, proportionellt och kostnadseffektivt, och det måste respektera de grundläggande rättigheterna. Den analys som kommissionen har genomfört och som beskrivs ovan och i konsekvensbedömningen visar att vart och ett av de genomförbara alternativen har både fördelar och nackdelar. Kommissionen har emellertid såsom förklaras ovan inte beaktat de alternativ som inte är genomförbara.

Mot bakgrund av den information som inhämtats är det i detta skede inte uppenbart att det finns skäl att lägga fram ett förslag om ett EU-system för att spåra finansiering av terrorism.

Kommissionen ser fram emot Europaparlamentets och rådets synpunkter på detta meddelande.