



EUROPA-KOMMISSIONEN

Bruxelles, den 13.7.2011
KOM(2011) 429 endelig

**MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET,
DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG
REGIONSUDVALGET**

Et europæisk system til sporing af finansiering af terrorisme: løsningsmodeller

**MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET,
DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG
REGIONSUDVALGET**

Et europæisk system til sporing af finansiering af terrorisme: løsningsmodeller

1. INDLEDNING

Da Rådet besluttede at indgå aftalen mellem Den Europæiske Union og Amerikas Forenede Stater om behandling og overførsel af finansielle betalingsdata fra Den Europæiske Union til USA til brug for programmet til sporing af finansiering af terrorisme (TFTP-aftalen mellem EU og USA)¹, opfordrede det også Kommissionen til at fremlægge "en juridisk og teknisk ramme for udtræk af data på EU's område" for Europa-Parlamentet og Rådet senest et år efter aftalens ikrafttrædelsesdato². Europa-Parlamentet har også løbende krævet, at der på længere sigt overvejes en varig, juridisk forsvarlig europæisk løsning på spørgsmålet om udtræk af data, der er anmodet om, på europæisk område³. Meddelelsen "Strategien for EU's indre sikkerhed i praksis - Fem skridt hen imod et mere sikkert EU" havde også allerede fastslået, at Kommissionen ville formulere en EU-politik til udtræk og analyse af oplysninger om finansielle transaktioner på europæisk område⁴. Med henvisning til de gode resultater, der er opnået med USA's TFTP, forventes det, at et europæisk system vil kunne bidrage mærkbart til at afskære terrorister fra adgang til finansiering og materiel, og det vil gøre det muligt at overvåge deres transaktioner. Der henvises også til artikel 11 i TFTP-aftalen mellem EU og USA, hvori det hedder, at Europa-Kommissionen i denne aftales løbetid gennemfører 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. Denne meddelelse er den første etape i Kommissionens opfølgning på denne artikel og på Rådets opfordring. Den beskriver de forskellige skridt, som Kommissionen skal tage i retning af at etablere en sådan "juridisk og teknisk ramme", og fremlægger de forskellige løsningsmuligheder, der kan overvejes for at nå dette mål. Den angiver ikke på nuværende tidspunkt nogen foretrukken løsning, men fremlægger dog de relevante spørgsmål, der skal tages i betragtning i forbindelse med de overvejede muligheder. Da spørgsmålet har stor politisk betydning og er juridisk og teknisk komplekst, ønsker Kommissionen at orientere Rådet og Europa-Parlamentet om situationen og indlede en debat. Kommissionen finder en sådan debat nyttig, inden den fremsætter konkrete forslag grundlag af en konsekvensanalyse.

Det bør i den forbindelse understreges, at denne meddelelse ikke indvirker på det forslag, Kommissionen vil fremlægge. Der vil med ethvert fremtidigt forslag blive taget hensyn til de ovennævnte drøftelser og den konsekvensanalyse, der vil blive foretaget på grundlag af en undersøgelse, som Kommissionen gav i underentreprise i andet halvår 2010. På grund af de følger, som et forslag til lovgivning ville få for de grundlæggende rettigheder, herunder navnlig databaseskyttelse, vil man i forbindelse med konsekvensanalysen især være opmærksom på, at eventuelle foranstaltninger, som Kommissionen måtte foreslå, skal være

¹ EUT L 195 af 27.7.2010, s. 5.

² Rådet afgørelse af 13. juli 2010 (EUT L 195 af 27.7.2010, s. 3).

³ Jf. f.eks. beslutning P7_TA(2010)0143 og begrundelsen i henstilling A7-0224/2010.

⁴ KOM(2010) 673 endelig af 22.11.2010. Se foranstaltning 2 under målsætning 2, s. 8

nødvendige og rimelige. Kommissionen vil til det formål følge de retningslinjer, der er formuleret i dens meddelelse om strategien for Den Europæiske Unions effektive gennemførelse af chartret om grundlæggende rettigheder.⁵

Derudover vil konsekvensanalysen tilvejebringe det nødvendige tekniske baggrundsmateriale samt en detaljeret vurdering af alle løsningsmuligheder. Disse spørgsmål er allerede blevet drøftet med mange interessenter på dette område, herunder medlemsstaternes myndigheder, databeskyttelsesmyndighederne, Europol og den udpegede udbyder. De endelige resultater af ovennævnte undersøgelse vil først være til rådighed i slutningen af året. For at støtte udarbejdelsen af konsekvensanalysen har Europa-Kommissionen afholdt tre ekspertmøder med de samme interessenter samt med de amerikanske myndigheder, der er involveret i gennemførelsen af TFTP. De løsningsmuligheder, der gennemgås i denne meddelelse, bygger på de foreløbige resultater af undersøgelsen og drøftelserne på disse ekspertmøder.

2. MÅLENE MED ETABLERINGEN AF ET EU-SYSTEM TIL SPORING AF FINANSIERING AF TERRORISME

Der er to hovedgrunde til at etablere et EU-system til sporing af finansiering af terrorisme (TFTS):

- systemet skal yde et effektivt bidrag til bekæmpelsen af terrorisme og finansieringen heraf i Den Europæiske Union
- systemet skal bidrage til at begrænse omfanget af personoplysninger, der overføres til tredjelande. Systemet bør omfatte behandling af de data, der er nødvendige for, at det kan gennemføres på EU's område med forbehold af EU's principper og lovgivning vedrørende databeskyttelse.

I USA har programmet til sporing af finansiering af terrorisme (TFTP) vist sig at tilføre bekæmpelsen af terrorisme og finansieringen heraf betydelig merværdi og ikke kun at være til gavn for de amerikanske myndigheder, men også for Den Europæiske Unions medlemsstater og tredjelande. Den seneste revision af TFTP-aftalen mellem EU og USA⁶ bekræftede, at siden TFTP blev indført i USA, er mere end 2 500 rapporter videreformidlet til myndighederne i tredjelande, og at langt størstedelen af disse rapporter (1 700) er blevet videreformidlet til Den Europæiske Union. Effekten af det amerikanske program og dets værdi for bekæmpelsen af terrorisme og finansieringen heraf er også blevet bekræftet i to rapporter fra dommer Bruguière, som Europa-Kommissionen i 2008 udpegede til at gennemgå programmet. De oplysninger, der var udledt af TFTP, og som blev stillet til rådighed for EU's myndigheder, omfattede vigtige spor i forbindelse med en række (forsøg på) terrorangreb med stor symbolværdi, såsom angrebene i Madrid og London, sammensværgelsen i 2006 med det formål at sprænge transatlantiske fly i luften ved hjælp af flydende sprængstoffer og forsøget i 2007 på at angribe amerikanske interesser i Tyskland. EU's revisionshold konkluderede også, at det havde modtaget overbevisende tilkendegivelser om TFTP's merværdi for bekæmpelsen af terrorisme og finansieringen heraf. På grund af disse erfaringer er der gode grunde til at tro, at et TFTS-system på EU-plan også vil have stor merværdi for EU's og medlemsstaternes bestræbelser på at bekæmpe terrorisme og finansieringen heraf.

⁵ KOM(2010) 573 endelig af 19.10.2010.

⁶ SEK(2011) 438 endelig af 30.3.2011.

Mens der ikke hersker nogen tvivl om effektiviteten af det amerikanske TFTP-program for bekæmpelsen af terrorisme og finansieringen heraf, er der blevet rejst alvorlig tvivl om følgerne for borgernes grundlæggende rettigheder. Disse bekymringer vedrører hovedsagelig den omstændighed, at gennemførelsen af TFTP-aftalen mellem EU og USA medfører, at der videregives et stort antal personoplysninger ("massedata") til de amerikanske myndigheder, hvoraf størstedelen vedrører borgere, der intet har at gøre med terrorisme eller finansieringen heraf. Sådanne data meddeles i form af massedata (på grundlag af relevante datakategorier) i stedet for på individuel basis (som svar på en anmodning vedrørende en eller flere enkeltpersoner), fordi udbyderen af disse data ikke har teknisk kapacitet til at fremskaffe dataene på et individuelt grundlag. Hvis udbyderen skulle meddele sådanne oplysninger på et individuelt grundlag, ville han skulle oprette en dedikeret søge- og analysefunktion, der ikke er nødvendig i forbindelse med hans forretningsmæssige praksis, og som ville kræve betydelige ressourcer. Anmodning om oplysninger på et individuelt grundlag ville også betyde, at udbyderen reelt ville blive klar over, hvilke enkeltpersoner der er genstand for efterforskninger af terrorhandlinger, og deres finansielle forbindelser. Dette kunne få indvirkning på sådanne efterforskningers effektivitet.

For at opvejere ulemperne ved meddelelse af masseoplysninger er der indført betydelige beskyttelsesforanstaltninger for at sikre, at der ikke kan finde misbrug af oplysninger sted, herunder at de meddelte oplysninger kun kan søges og anvendes til bekæmpelse af terrorisme og finansieringen heraf. Den seneste gennemgang af TFTP-aftalen mellem EU og USA bekræftede, at disse beskyttelsesforanstaltninger faktisk er gennemført i overensstemmelse med bestemmelserne i aftalen.

Det er dog blevet anført, at videregivelsen af så store mængder personoplysninger til et tredjeland udgør en uberettiget krænkelse af disse borgeres grundlæggende rettigheder under hensyntagen til nødvendigheden og forholdsmæssigheden af denne krænkelse. Derfor opfordrede Rådet Kommissionen til at fremlægge forslag til etablering af et system for udtræk af sådanne data på EU's område. Det overordnede mål er at sikre, at behandlingen af sådanne data finder sted i overensstemmelse med EU's lovgivning og principper vedrørende databeskyttelse og EU's charter om grundlæggende rettigheder. Det skal i den forbindelse bemærkes, at de offentlige myndigheders indsamling og behandling af finansielle betalingsdata berører retten til beskyttelse af personoplysninger, jf. artikel 16 i TEUF og artikel 8 i chartret.

I overensstemmelse med artikel 52, stk. 1, i chartret skal enhver begrænsning af disse grundlæggende rettigheder være lovbestemt, den skal være tilstrækkeligt præcis samt af en sådan art, at den sikrer forudseelighed, og grundprincipperne i disse rettigheder skal være overholdt. Den må desuden ikke gå ud over, hvad der er nødvendigt og rimeligt, for at opfylde et legitimt mål, der er anerkendt af Unionen. Der skal derfor ikke blot tages hensyn til disse principper, når der træffes afgørelse om eventuel indførelse af et TFTP-system på EU-plan, men også til de forskellige muligheder, der er for gennemførelsen af systemet. Derfor berører disse principper også de valg, der skal træffes med hensyn til spørgsmål som systemets omfang, de lagringsperioder, der gælder, og den enkeltes ret til aktindsigt og sletning af oplysninger. Disse spørgsmål er ikke behandlet i enkeltheder i denne meddelelse. De vil skulle analyseres fuldt ud i konsekvensanalysen.

Den eventuelle indførelse af et system for udtræk af data på EU's område ville naturligvis få konsekvenser for den eksisterende TFTP-aftale mellem EU og USA, jf. artikel 11, stk. 3, i aftalen, hvori det hedder, at da etableringen af et EU-system i væsentlig grad kan ændre baggrunden for denne aftale, bør parterne høres for at afgøre, om der er behov for at tilpasse

denne aftale, hvis Den Europæiske Union beslutter at etablere et sådant system. Alle muligheder ville derfor indvirke på den fremtidige gennemførelse og efterfølgende tilpasning af den eksisterende TFTP-aftale mellem EU og USA.

3. DE VIGTIGSTE FUNKTIONER I ET EU-SYSTEM TIL SPORING AF FINANSIERING AF TERRORISME

Noget af det første, der kom frem under drøftelserne med ovennævnte interessenter, er, at disse interessenter overvejende er af den opfattelse, at hvis der skal etableres et EU-system til sporing af finansiering af terrorisme (EU-TFTS), bør det være med det formål at skabe sikkerhed for EU's borgere. Systemet bør ikke oprettes for at give relevante oplysninger til de amerikanske myndigheder. Medlemsstaternes myndigheder har ligeledes en reel interesse i resultater der opnås med et sådant system. Denne tilgang indebærer også, at selv om det amerikanske TFTP sikkert kunne give inspiration til, hvordan et sådant system kunne oprettes, ville en europæisk pendant hertil ikke nødvendigvis skulle kopiere alle elementer i det amerikanske TFTP-program. Endvidere skulle et EU-system oprettes under hensyn til de særlige forhold, der kendetegner EU's juridiske og administrative ramme, herunder respekt for de gældende grundlæggende rettigheder som anført ovenfor.

Ethvert system, der har til formål at spore finansiering af terrorisme i overensstemmelse med de hovedmål, der er skitseret ovenfor, skal dog indebære gennemførelse af følgende centrale funktioner:

- forberedelse og udstedelse af (juridisk gyldige) anmodninger til den(de) udpegede udbyder(e) af finansielle betalingstjenester om de rådata, der skal stilles til rådighed for en eller flere godkendte modtagere. Dette indebærer fastlæggelse af de kategorier af betalingsdata, der skal anmodes om, hvor ofte disse data skal sendes, og opretholdelse af kontakter med udbyderne vedrørende disse spørgsmål
- tilsyn med og godkendelse af anmodninger til den(de) udpegede udbyder(e) om sådanne rådata. Dette indebærer kontrol af, om anmodningen om sådanne rådata er blevet udarbejdet i overensstemmelse med de gældende begrænsninger
- modtagelse og lagring (behandling) af rådata fra den(de) udpegede udbyder(e), herunder implementering af et passende system for fysisk og elektronisk datasikkerhed
- gennemførelse af de faktiske søgninger i de leverede data i overensstemmelse med det gældende retsgrundlag, ud fra anmodninger om sådanne søgninger fra myndigheder i medlemsstaterne, USA eller andre tredjelande på grundlag af klart definerede betingelser og sikkerhedsforanstaltninger eller på initiativ af den (de) myndighed(er), der har ansvaret for databehandling
- tilsyn med og godkendelse af gennemførelsen af søgninger i de leverede data
- analyse af resultaterne af søgningerne ved at kombinere disse resultater med andre tilgængelige oplysninger eller efterretninger
- formidling af resultaterne af søgningerne (uden yderligere analyse) eller resultaterne af analyserne til de godkendte modtagere

- gennemførelse af en passende databeskyttelsesordning, herunder gældende lagringsperioder, logningsforpligtelser, behandling af anmodninger om adgang, berigtigelse og sletning osv.

Disse centrale funktioner skal fastsættes i passende retsakter på EU-niveau, på nationalt niveau eller på begge niveauer, afhængigt af hvilken mulighed der er valgt.

4. NØGLEPRINCIPPER VED OVERVEJELSE AF LØSNINGSMULIGHEDER

Ud over overvejelserne om de ovenfor beskrevne centrale funktioner vil valget mellem løsningsmulighederne i vidt omfang afhænge af, hvilke resultater de giver med hensyn til en række nøglespørgsmål, der for øjeblikket overvejes i forbindelse med konsekvensanalysen, og som gennemgås i det følgende.

4.1. Effektivitet

Den forventede effektivitet af de forskellige løsningsmuligheder i forbindelse med opfyldelsen af det centrale mål, nemlig at bekæmpe terrorisme og finansieringen heraf, er en afgørende faktor. Løsninger, der øger mulighederne for datadeling og -analyse på internationalt plan, bør fremmes ud fra denne synsvinkel, da en sådan datadeling og -analyse vil øge effektiviteten og tilføre større merværdi. I den forbindelse vil valget af organisation(er), der får til opgave at analysere dataene, og videreformidling af analyseresultaterne til de berørte myndigheder have stor betydning for systemets effekt og antallet af data, der overføres. Alligevel bør medlemsstaterne i overensstemmelse med den nuværende praksis fortsat have fuld kontrol over, om deres oplysninger eller efterretninger kan deles med andre myndigheder.

4.2. Databeskyttelse

International deling og analyse af oplysninger og efterretninger kan kun finde sted inden for en solid og veludviklet databeskyttelsesramme. Effektiviteten af en sådan ramme afhænger ikke kun af de relevante retsregler, der sætter de registrerede i stand til at udøve deres rettigheder til f. eks. domstolsprøvelse, men også af, om der er erfarent personale til rådighed, såsom en uafhængig databeskyttelsesansvarlig og en uafhængig og erfaren databeskyttelseskontrolmyndighed. Nogle af de organisationer, der kunne blive inddraget i den mulige etablering af et TFTS-system på EU-plan, råder allerede over sådanne strukturer, mens disse for andres vedkommende først skal oprettes. Derfor skal de databeskyttelsesmæssige konsekvenser af hver af de forskellige løsningsmuligheder først vurderes nøje i overensstemmelse med de overordnede principper vedrørende respekt for de grundlæggende rettigheder, der er omhandlet i afsnit 2 i denne meddelelse.

4.3. Datasikkerhed

Strengt databeskyttelsesbestemmelser skal kombineres med den mest avancerede datasikkerhedsinfrastruktur og -teknologi. Datasikkerhedsovervejelser peger i retning af at begrænse antallet af steder, hvor de leverede data kan behandles, samt at begrænse enhver form for adgang til dataene udefra. Den sikreste løsning ville være lagring ét sted uden adgang udefra. De fleste af de organisationer, der kunne inddrages i driften af TFTS-systemet, råder allerede over sikre databehandlingsteknologier, men ikke alle har på nuværende tidspunkt kapacitet til at behandle data, der er klassificeret over niveauet "EU Restricted".

4.4. Lagring af data

Lagringen af data bør finde sted enten på nationalt plan eller EU-plan. På EU-plan kunne lagring af data, der er modtaget fra den(de) udpegede udbyder(e), finde sted i Europol eller et andet EU-organ f.eks. agenturet for den operationelle forvaltning af store it-systemer inden for området frihed, sikkerhed og retfærdighed (IT-agenturet)⁷, der er ved at blive oprettet. Da lagring af data er uløseligt forbundet med spørgsmålene om databeskyttelse og datasikkerhed, bør valget af den organisation, der er ansvarlig for lagringen af dataene, være tæt knyttet til den ordning for databeskyttelse og datasikkerhed, som disse organisationer kan tilbyde.

4.5. Udnyttelse af de eksisterende strukturer og instrumenter

Alle løsningsmuligheder bør så vidt muligt udnytte de eksisterende strukturer. Det begrænser omkostningerne og gør det muligt at drage nytte af den indhøstede erfaring samt den eksisterende infrastruktur. En sådan udnyttelse af eksisterende instrumenter kræver, at nye opgaver, der overdrages en eksisterende organisation, passer godt til denne organisations eksisterende mandat. Europol, Eurojust eller nationale retlige myndigheder kan eventuelt kontrollere og godkende de anmodninger om udlevering af data, der rettes til den(de) udpegede udbyder(e).

4.6. Samarbejdet mellem de kompetente myndigheder

De løsningsmuligheder, der er skitseret nedenfor, indebærer forskellige grader af samarbejde og deling af oplysninger og efterretninger mellem de nationale myndigheder indbyrdes og mellem de nationale myndigheder og EU's myndigheder. Forskellige medlemsstater har fastsat forskellige måder, hvorpå deres nationale myndigheder samarbejder om bekæmpelsen af terrorisme, og enhver aktion på EU-plan skal respektere de begrænsninger, der er fastsat i artikel 72 i TEUF vedrørende medlemsstaternes beføjelser med hensyn til opretholdelse af lov og orden og beskyttelse af den indre sikkerhed. Ethvert EU-TFTS skal derfor gøre det muligt for medlemsstaterne at udøve betydelig kontrol med de oplysninger og efterretninger, som de er rede til at dele inden for rammerne af et sådant system. En række af nedennævnte organisationer har udviklet forskellige tilgange til dette spørgsmål, hvoraf nogle vil kunne anvendes direkte på det system, der skal indføres.

4.7. Et første generelt overblik over de finansielle konsekvenser af de forskellige løsninger

De samlede omkostninger til etableringen af et TFTS-system på EU-plan og deres fordeling mellem EU og medlemsstaterne vil i vidt omfang afhænge af, hvilken politik der vælges. Omkostningerne vil under alle omstændigheder omfatte:

- omkostninger i forbindelse med sikker overførsel og lagring af data fra den(de) udpegede udbyder(e)
- Omkostninger i forbindelse med udviklingen og vedligeholdelsen af den software, der er nødvendig for gennemførelse af søgninger og tilrådsstilling af søgeresultater
- omkostninger i forbindelse med formidling af søgeresultater eller analyser til godkendte modtagere

⁷ KOM(2010)93 endelig af 19.3.2010.

- omkostninger til det personale, der foretager søgninger og analyse og formidler resultaterne heraf
- omkostninger til personale med ansvar for tilsyns- og revisionsopgaver
- omkostninger til personale med ansvar for databeskyttelse og borgernes rettigheder.

Selv om der endnu ikke er detaljerede overslag til rådighed, viser foreløbige beregninger, at omkostningerne til den rene EU-løsning og alle de forskellige hybridløsninger, der gennemgås i det følgende, vil ligge i størrelsesordenen 33-47 mio. EUR til oprettelse og yderligere 7-11 mio. EUR til den årlige drift. I afsnit 6 i denne meddelelse beskrives forskellige løsninger. Løsning 3 vil være den dyreste med 43 mio. EUR i etableringsomkostninger for EU og 3,7 mio. EUR for medlemsstaterne (kombineret) og med 4,2 mio. EUR i årlige driftsomkostninger for EU og 6,8 mio. EUR for medlemsstaterne (kombineret). Løsning 2 ville være den billigste med 33 mio. EUR i etableringsomkostninger for EU og 3,5 mio. EUR i årlige driftsomkostninger på EU-plan samt 3,3 mio. EUR i årlige driftsomkostninger for medlemsstaterne (kombineret). Løsning 1 ville kræve 40,5 mio. EUR i etableringsomkostninger for EU og 4 mio. EUR i årlige driftsomkostninger på EU-plan samt 5 mio. EUR i årlige driftsomkostninger for medlemsstaterne (kombineret). Disse omkostninger vil naturligvis blive reduceret, hvis der kan trækkes på personalet i eksisterende organisationer, eller hvis man kan anvende de eksisterende infrastrukturer samt eksisterende soft- og hardware. Omkostningerne til etablering og drift af et rent nationalt system ville være betydeligt højere (390 mio. EUR i etableringsomkostninger og 37 mio. EUR i årlige driftsomkostninger), da alle medlemsstater i så fald skulle etablere højsikrede databehandlingssystemer og have personale ansat til at drive systemet.

Disse beløb er foreløbige og vil skulle analyseres og præciseres yderligere på baggrund af resultatet af konsekvensanalysen.

5. SPØRGSMÅL, DER SKAL TAGES I BETRAGTNING

Uanset valget mellem de forskellige løsninger for etablering og drift af et TFTS-system på EU-plan er det nødvendigt at tage en række relevante spørgsmål i betragtning vedrørende omfanget af et muligt TFTS-system på EU-plan. Disse gennemgås i det følgende.

5.1. Terrorisme og finansiering heraf eller et bredere anvendelsesområde?

Adgangen til finansielle betalingsdata er ikke kun nyttig for bekæmpelsen af terrorisme og finansieringen heraf. Der er ikke megen tvivl om, at en sådan adgang også vil være et værdifuldt redskab for bekæmpelsen af andre former for grov kriminalitet, navnlig organiseret kriminalitet og hvidvaskning af penge. I forbindelse med TFTP-aftalen mellem EU og USA har overvejelser om forholdsmæssighed dog ført til en streng begrænsning af brugen af dataene til bekæmpelse af terrorisme og finansieringen heraf. De foreløbige drøftelser, der har fundet sted indtil nu, viser, at der er bred enighed om, at sådanne overvejelser om forholdsmæssighed også peger i retning af at indføre samme begrænsede anvendelsesområde for et tilsvarende europæisk system i overensstemmelse med de generelle betragtninger vedrørende respekten for de grundlæggende rettigheder, der er omhandlet i afsnit 2 i denne meddelelse.

5.2. Mere end én udbyder?

TFTP-aftalen mellem EU og USA er på nuværende tidspunkt begrænset til anmodninger om data fra én udbyder af internationale finansielle betalingstjenester. Selv om denne udbyder klart er den vigtigste udbyder af sådanne betalingstjenester på verdensplan, er der også andre udbydere på markedet. Overvejelser om effektivitet og skabelse af lige vilkår for alle aktører på dette marked peger i retning af at etablere et system, der gælder for alle udbydere af internationale finansielle betalingstjenester. Under alle omstændigheder skal der tages hensyn til den administrative byrde for virksomheder, der stiller finansielle betalingstjenester til rådighed, ved valget af de løsningsmuligheder, der er til rådighed.

5.3. Kun internationale betalingstjenester eller også nationale?

TFTP-aftalen mellem EU og USA er på nuværende tidspunkt begrænset til anmodninger om data fra udbydere af internationale finansielle betalingstjenester, dvs. betalingstjenester, som anvendes til gennemførelse af transnationale transaktioner, bl.a. mellem EU-medlemsstaterne, men undtaget er meddelelser om finansielle transaktioner vedrørende det fælles eurobetalingsområde (SEPA). Med et EU-TFTS skal det også vurderes, hvorvidt det skal omfatte meddelelser om finansielle transaktioner, der udveksles mellem medlemsstaterne, eller om det skal begrænses til international udveksling af tjenesteydelser vedrørende sådanne meddelelser. Rent nationale finansielle tjenester (der kun anvendes i forbindelse med nationale finansielle transaktioner) er på nuværende tidspunkt ikke omfattet af TFTP-aftalen mellem EU og USA. Adgangen til sådanne nationale finansielle betalingstjenester ville være af interesse for bekæmpelsen af terrorisme og andre former for kriminalitet. Men selv om man lod spørgsmålet om, hvorvidt adgangen til sådanne rent nationale transaktioner skal reguleres på EU-plan, ligge, bekræftede de foreløbige drøftelser den opfattelse, at denne adgang i vidt omfang anses for at være ude af proportion og derfor bør udelukkes fra et EU-system.

5.4. Hvilken type finansielle betalingsdata skal omfattes?

Der er mange forskellige typer finansielle betalingsdata, som anvendes i det internationale banksystem. TFTP-aftalen mellem EU og USA er på nuværende tidspunkt begrænset til én bestemt type finansielle betalingsdata. Adgangen til andre typer finansielle betalingsdata ville være af interesse for bekæmpelsen af terrorisme og finansieringen heraf og eventuelt andre former for kriminalitet. Også med hensyn til dette valg peger overvejelser om forholdsmæssighed og respekt for borgernes grundlæggende rettigheder dog i retning af at begrænse omfanget af de typer af finansielle betalingsdata, der skal være omfattet af systemet. Nærmere enkeltheder om dette tekniske spørgsmål vil blive medtaget i konsekvensanalysen.

6. LØSNINGSMULIGHEDER FOR ET TFTS-SYSTEM PÅ EU-PLAN

De nedenfor beskrevne løsningsmuligheder gennemgås i øjeblikket af Kommissionen som led i den løbende konsekvensanalyse. De er ikke nødvendigvis udtømmende og foregriber på ingen måde den endelige konsekvensanalyse eller det valg, som Kommissionen vil træffe på grundlag heraf.

En af de løsninger, der altid overvejes i forbindelse med forberedelsen af nye initiativer og deres ledsagende konsekvensanalyser, er muligheden af at bevare status quo, hvilket i dette tilfælde ville betyde, at man lod TFTP-aftalen mellem EU og USA være, som den er, og ikke fremsatte noget forslag om et EU-TFTS. Denne løsningsmodel ville ikke imødekomme opfordringen fra Rådet og Parlamentet til Kommissionen om at forelægge et nyt forslag om

"en juridisk og teknisk ramme for udtræk af data på EU's område", som er omhandlet i afsnit 1 i denne meddelelse. Derudover ville denne løsning ikke bidrage til at begrænse den mængde personoplysninger, der overføres til tredjelande, og den ville ikke muliggøre behandling af data på EU's område i overensstemmelse med EU's principper og lovgivning vedrørende databeskyttelse. De andre løsningsmodeller, der gennemgås mere i detaljer nedenfor, giver alle mulighed for at etablere et TFTS-system på EU-plan.

Teoretisk set kunne alle de kernefunktioner, der er indkredset i en EU-TFTS som beskrevet i afsnit 3 i denne meddelelse, gennemføres enten på EU-plan eller på nationalt plan. Funktionerne kan også overlades til en eller flere forskellige organisationer inden for rammerne af deres eksisterende ansvarsområder, eller der kunne oprettes nye organisationer til at udføre dem. Sådanne organisationer kunne enten være på EU-plan eller på nationalt plan. Dette indebærer, at en rent EU-baseret model – også i teorien – er mulig, hvor alle kernefunktioner ville blive overladt til organisationer på EU-plan, ligesom en rent national model, hvor alle funktioner ville blive udført på nationalt plan, også er mulig. Generelt bør man også holde sig for øje, at valgene mellem et centraliseret eller decentraliseret system eller et hybridsystem i dette særlige tilfælde ikke nødvendigvis er de samme som de valg, der træffes med hensyn til andre initiativer, som indebærer databehandling med henblik på bekæmpelse af terrorisme og finansieringen heraf. Hvert initiativ på dette område bør bedømmes individuelt.

Både rent centraliserede og rent nationale tilgange er forbundet med betydelige ulemper. F.eks. ville en rent EU-baseret model sikkert lide under, at den ikke ville have nogen forbindelse med medlemsstaternes retshåndhævende organisationer og efterretningsorganisationer samt praksis, og derfor ikke være særlig effektiv. Uden input fra de nationale myndigheder med ansvar for behandling af disse spørgsmål ville det være næsten umuligt præcist at fastlægge, hvilke kategorier af data der skulle anmodes om fra den(de) udpegede udbyder(e). Nyttens af systemet ville også blive reduceret, hvis søgninger i databasen kun fandt sted på grundlag af efterretninger, som er tilgængelige på EU-plan. Med EU's nuværende integrationsniveau er sådanne efterretninger i vidt omfang kun tilgængelige på nationalt plan. Det er heller ikke sandsynligt, at medlemsstaterne ville acceptere en sådan rent EU-baseret tilgang, da den ikke ville tilføre nogen merværdi for deres egne bestræbelser på at bekæmpe terrorisme og finansieringen heraf. Under konsultationerne oplyste medlemsstaterne også, at denne løsningsmodel ville være politisk vanskelig at acceptere af juridiske og operationelle grunde.

I det andet yderpunkt ville der være en risiko for, at en rent national tilgang ville blive gennemført forskelligt i de forskellige medlemsstater, og en øget risiko for brud på datasikkerheden, da det er nødvendigt at råde over 27 forskellige kopier af de leverede data. En rent national tilgang ville også volde problemer i relation til gennemførelsen af en harmoniseret databeskyttelsesramme samt en harmoniseret tilgang til (kontrollen med) andre nødvendige begrænsninger såsom begrænsningen til terrorisme og finansieringen heraf. Med en rent national tilgang er det endvidere uklart, hvilken medlemsstat der ville være ansvarlig for behandlingen af anmodninger om søgninger fra tredjelande, og den ekstra gevinst ved en analyse af søgeresultaterne på EU-plan ville gå tabt. Derudover ville omkostningerne i forbindelse med denne løsningsmulighed som påpeget ovenfor være væsentligt højere, da alle medlemsstater i så fald skulle indføre højsikrede databehandlingssystemer og have personale ansat til at drive systemet.

Det forberedende arbejde med interessenterne viste hurtigt, at der ikke var opbakning til de løsninger, der ligger i yderpolerne af spektret af løsningsmuligheder. Der var enighed om, at en hybridløsning, der indebærer en fordeling af de forskellige funktioner på forskellige

organisationer på EU-plan og nationalt plan, sandsynligvis ville give de bedste resultater for de to hovedmål. Selv om denne enighed hjælper med at finde frem til den mest egnede løsning, indebærer hybridløsningen fortsat, at der skal træffes et stort antal valg. I nedenstående afsnit beskrives de tre hybridløsninger, der er resultatet af det igangværende forberedende arbejde, i lidt mere detaljeret form som de mest troværdige. Løsningsmulighederne vises også i tabelform i bilaget.

6.1. Koordinationstjenesten og den analytiske tjeneste under TFTS-systemet på EU-plan (model 1)

Denne løsningsmodel ville indebære oprettelse af en central TFTS-enhed på EU-plan med de fleste af de opgaver og funktioner, der gennemføres på EU-plan. Udstedelse af anmodninger om "rådata" til den(de) udpegede udbyder(e), verifikation af disse anmodninger, behandling af anmodninger om søgninger og gennemførelse heraf, forvaltning af søgeresultater og fremsendelse af rapporter til dem, der har anmodet om søgninger, ville alt sammen finde sted på EU-plan. Udarbejdelse af anmodninger til den(de) udpegede udbyder(e) kunne dog finde sted i samråd med de kompetente myndigheder i medlemsstaterne, og medlemsstaterne kunne også vælge at udstationere deres egne analytikere i den centrale enhed, så de kunne deltage i gennemførelsen af søgningerne. I modsætning til den fuldt centraliserede model kunne medlemsstaterne anmode om, at der gennemføres søgninger på deres vegne, svarende til den nuværende procedure inden for rammerne af det amerikanske TFTP-program, eller at søgningerne gennemføres af deres egne analytikere.

Medlemsstaterne skulle i så fald dele oplysninger med EU's centrale TFTS-enhed, "begrunde" anmodningen og dens sammenhæng med terrorisme, inden en søgning kunne iværksættes, eller få deres anmodninger "forhåndsgodkendt" af de nationale myndigheder. Sådanne nationale myndigheder kunne f.eks. være nationale offentlige anklagere eller undersøgelsesdommere inden for terrorbekæmpelse. Hvis de ville godkende en bestemt søgning i de udleverede data, kunne EU's centrale TFTS-enhed acceptere at udføre sådanne søgninger uden yderligere kontrol. Med dette scenarie ville det ikke være nødvendigt at stille yderligere efterretninger til rådighed for EU's centrale TFTS-enhed. EU's centrale TFTS-enhed ville så fremsende resultaterne af søgningerne og analysen heraf og kunne også meddele oplysninger uopfordret. USA og andre tredjelande ville også skulle anmode om gennemførelse af søgninger efter en lignende procedure.

Kontrollen af overensstemmelsen med beskyttelses- og kontrolforanstaltningerne ville også blive centraliseret, eventuelt overvåget af eksterne interessenter, der f.eks. repræsenterer den(de) udpegede udbyder(e) og dem, der er udpeget som uafhængige tilsynsførende. Databeskyttelse, dataintegritet og datasikkerhed ville også blive sikret på centralt plan.

De vigtigste organer, der skal involveres i systemet, kunne være Europol og Eurojust. De opgaver, der skal udføres af Europol og Eurojust, må i så fald være i overensstemmelse med deres opgaver som fastsat i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Det skal også fastlægges, hvorvidt de retsakter, der på nuværende tidspunkt regulerer deres funktion, skal ændres. Hvis Europol blev valgt som EU's centrale TFTS-myndighed, skulle den også tage sig af anmodninger fra registrerede personer om adgang, sletning og blokering, alt sammen i overensstemmelse med gældende retsgrundlag og databeskyttelsesbestemmelser. EU's centrale TFTS-enhed ville udføre sin rolle i overensstemmelse med det gældende retsgrundlag, og sager om domstolsprøvelse og administrativ prøvelse ville ligeledes blive behandlet i overensstemmelse med gældende retsregler. På nationalt plan ville de nationale retshåndhævende myndigheder blive inddraget for at kontrollere og godkende anmodninger

om søgninger. Muligheden for at oprette nye nationale organer kunne overvejes, men dette valg overlades bedst til medlemsstaterne på grundlag af subsidiaritetsprincippet⁸.

6.2. EU's TFTS-tjeneste for udtræk af data (model 2)

Som det var tilfældet med den første politiske løsningsmodel, ville denne løsning indebære, at der oprettes en central TFTS-enhed på EU-plan, der bl.a. skulle have til opgave at udstede anmodninger om "rådata" til den(de) udpegede udbyder(e), verifikation af disse anmodninger og behandling af anmodninger om søgninger. EU's TFTS-enhed ville dog i forbindelse med denne løsningsmodel ikke få tilladelse til at analysere søgeresultaterne og sammenligne dem med andre tilgængelige oplysninger eller efterretninger, når sådanne søgninger foretages på anmodning af myndighederne i medlemsstaterne. I sådanne tilfælde ville dens rolle være begrænset til at forberede og formidle søgeresultaterne på en overskuelig måde.

Som i forbindelse med løsning nr. 1, ville anmodninger om "rådata", der skal udstedes til den(de) udpegede udbyder(e), blive udarbejdet i tæt samråd med medlemsstaterne, der kunne tilkendegives deres specifikke behov over for den centrale TFTS-enhed, som så ville analysere disse og fremsætte anmodning(en)(erne) på grundlag af denne analyse.

Medlemsstaternes myndigheder ville anmode om, at søgningerne foretages på deres vegne. Hvorvidt sådanne anmodninger er begrundede og har en sammenhæng med terrorisme, ville blive verificeret og godkendt på nationalt plan. EU's centrale TFTS-enhed ville udføre søgningen og levere hele resultatsættet til medlemsstaterne i en overskuelig form. Medlemsstaternes myndigheder ville være de eneste, som skulle analysere resultaterne, og de kunne også vælge at stille oplysninger til rådighed uopfordret.

EU's centrale TFTS-enhed ville få til opgave at gennemføre søgninger og analysere resultaterne på vegne af EU-institutioner, USA og andre tredjelande. Den kunne også uopfordret levere oplysninger på dette grundlag.

Som i forbindelse med de foregående løsningsmodeller ville kontrollen af overensstemmelsen med beskyttelses- og kontrolforanstaltningerne også blive centraliseret, eventuelt overvåget af eksterne interessenter, der f.eks. repræsenterer den(de) udpegede udbyder(e) og dem, der er udpeget som uafhængige tilsynsførende. Databeskyttelse, dataintegritet og datasikkerhed ville også blive sikret på centralt plan.

Som i forbindelse med de foregående løsningsmodeller kunne de vigtigste organer, der skal involveres i systemet, være Europol og Eurojust. På nationalt plan ville de vigtigste involverede organer være de nationale retshåndhævende myndigheder eller efterretningsmyndigheder. Som allerede nævnt vil det i overensstemmelse med subsidiaritetsprincippet være op til medlemsstaterne at afgøre, om der skal oprettes nye nationale organer. Europol og/eller de nationale enheder ville komme til at behandle anmodninger fra EU-borgere om adgang, berigtigelse og sletning, hvilket ville involvere både nationale databeskyttelsesmyndigheder og Europols fælles kontrolinstans. Sager om domstolsprøvelse og administrativ prøvelse ville blive behandlet i overensstemmelse med gældende retsregler på nationalt plan eller EU-plan⁹.

⁸ På nuværende tidspunkt er konsekvenserne for de EU-budgetter, der kunne komme til at spille en rolle i gennemførelsen af systemet, endnu ikke kendt.

⁹ Se fodnote 8.

6.3. Koordinationstjenesten under den finansielle efterretningsenhed (FIU) (model 3)

Denne politiske løsningsmodel ville indebære oprettelse af en opgraderet EU-plattform, eventuelt baseret på FIU-plattformen, som udgøres af FIU'er i medlemsstaterne. Ad hoc-myndigheden på EU-plan ville udstede anmodninger om "rådata" til den(de) udpegede udbyder(e) ved at samle de behov, som FIU'erne har angivet, i én enkelt anmodning, som også ville blive verificeret og godkendt på centralt plan.

Hver enkelt FIU ville være ansvarlig for gennemførelsen af søgningerne og forvaltningen af resultaterne på vegne af medlemsstaterne samt for gennemførelsen af analyser og fremsendelsen af rapporter til dem, den anser for relevante. Hvorvidt sådanne søgninger er begrundede og har en sammenhæng med terrorisme, ville blive verificeret og godkendt på nationalt plan. FIU'erne ville også være ansvarlige for den uopfordrede levering af oplysninger.

Den opgraderede FIU-plattform ville blive i stand til at gennemføre søgninger og analysere resultaterne på vegne af EU-institutionerne og tredjelande, med hvilke EU har undertegnet en aftale. Den kunne også levere oplysninger uopfordret.

Kontrollen af overensstemmelsen med beskyttelses- og kontrolforanstaltningerne ville blive centraliseret, eventuelt overvåget af eksterne interessenter, der f.eks. repræsenterer den(de) udpegede udbyder(e) og dem, der er udpeget som uafhængige tilsynsførende. Databeskyttelse, dataintegritet og datasikkerhed ville også blive sikret på centralt plan.

Den opgraderede FIU-plattform ville blive tildelt en formel juridisk status med klart definerede roller og ansvarsområder. På nationalt plan ville de vigtigste involverede organer være FIU'erne og de nationale retshåndhævende myndigheder eller efterretningsmyndigheder.

En EU-myndighed ville behandle anmodninger fra EU-borgere om adgang, berigtigelse og sletning, idet sager om domstolsprøvelse og administrativ prøvelse ville blive behandlet i overensstemmelse med gældende retsregler på nationalt plan og EU-plan.

7. KONKLUSION

På grundlag af Kommissionens hidtidige forberedende arbejde og med forbehold af resultaterne af konsekvensanalysen beskriver denne meddelelse de forskellige mulige løsninger til etablering af en "juridisk og teknisk ramme for udtræk af data på EU's område" som led i et system til sporing af finansiering af terrorisme. De forskellige løsningsmodeller, der er beskrevet i denne meddelelse, viser, at der stadig vil skulle træffes vigtige valg og afgørelser, herunder med hensyn til respekten for de grundlæggende rettigheder, og der skal gås meget mere i dybden med mange juridiske, tekniske, organisatoriske og finansielle spørgsmål under det videre forberedende arbejde. På grund af de betydelige udfordringer finder Kommissionen, at der er behov for tilstrækkelig tid til det videre forberedende arbejde og til drøftelser med Rådet og Parlamentet.

* * *

Bilag: Skematisk oversigt over hybridløsninger

	Koordinationstjenesten og den analytiske tjeneste under TFTS-systemet på EU-plan (model 1)	EU's TFTS-tjeneste for udtræk af data (model 2)	Koordinationstjenesten under den finansielle efterretningsenhed (FIU) (model 3)
Forberedelse og udstedelse af anmodninger om "rådata"	EU's centrale TFTS-enhed i samråd med medlemsstaterne	EU's centrale TFTS-enhed i samråd med medlemsstaterne	Opgraderet FIU-platform
Tilsyn med og godkendelse af anmodninger om "rådata"	Eurojust eller et andet eksisterende organ	Eurojust eller et andet eksisterende organ	Eurojust eller et andet eksisterende organ
Modtagelse og lagring af "rådata", datasikkerhed	Europol eller et andet EU-organ, såsom IT-agenturet	Europol eller et andet EU-organ, såsom IT-agenturet	Europol eller et andet EU-organ, såsom IT-agenturet
Gennemførelse af søgninger i "rådata"	EU's centrale TFTS-enhed, udstationerede analytikere fra medlemsstaterne eller en kombination heraf	EU's centrale TFTS-enhed	FIU'er, opgraderet FIU-platform
Tilsyn med og godkendelse af gennemførelsen af søgninger	Uafhængige tilsynsførende, evt. nationale myndigheder	Uafhængige tilsynsførende, nationale myndigheder	Uafhængige tilsynsførende
Analyse af resultaterne af søgningerne	EU's centrale TFTS-enhed, udstationerede analytikere fra medlemsstaterne eller en kombination heraf	Nationale myndigheder med ansvar for nationale søgninger, EU's centrale TFTS-analytikere for EU- og tredjelandssøgninger	Opgraderet FIU-platform, nationale FIU'er
Formidling af resultaterne af søgningerne	Europol-analytikere eller analytikere udstationeret af medlemsstaterne	Nationale myndigheder med ansvar for nationale søgninger, EU's centrale TFTS-analytikere for EU- og tredjelandssøgninger	Opgraderet FIU-platform, nationale FIU'er

Gennemførelse af en passende databeskyttelsesordning	Europol eller et andet EU-organ, såsom IT-agenturet	Europol eller et andet EU-organ, såsom IT-agenturet	Europol eller et andet EU-organ, såsom IT-agenturet
--	---	---	---