EUROPESE
COMMISSIE

Brussel, 27.11.2013
COM(2013) 842 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Een Europees systeem voor het traceren van terrorismefinanciering (EU-TFTS)

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

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Een Europees systeem voor het traceren van terrorismefinanciering (EU-TFTS)

Deze mededeling is een vervolg op die van 13 juli 2011 (COM(2011) 429) en heeft als doel het Europees Parlement en de Raad te informeren over de resultaten van de analyse die is verricht inzake de uitvoerbaarheid van een Europees systeem voor het traceren van terrorismefinanciering (EU-TFTS).

1. CONTEXT

1.1. Achtergrond van het verzoek en definitie

Tijdens de onderhandelingen die aan de sluiting van de TFTP-overeenkomst tussen de EU en de VS[1] voorafgingen, is besproken hoe in het kader van deze overeenkomst persoonsgegevens het best zouden kunnen worden beschermd en de grondrechten het best zouden kunnen worden nageleefd. Daarbij stelden sommige partijen dat extractie van gegevens op Europees grondgebied de hoeveelheid aan de VS door te geven gegevens zou beperken en derhalve een hoger niveau van gegevensbescherming zou waarborgen. Een aantal lidstaten beschouwde het als een toegevoegde waarde om op de lange termijn een onafhankelijk Europees systeem voor het traceren van terrorismefinanciering te ontwikkelen. Het Europees Parlement verzocht de Raad en de Commissie om alle nodige maatregelen te nemen om een duurzame, juridisch verantwoorde Europese oplossing te bieden voor het extraheren van de gevraagde gegevens op Europees grondgebied. Toen de Raad en het Europees Parlement met de sluiting van de TFTP-overeenkomst tussen de EU en de VS instemden, verzochten zij de Commissie om uiterlijk een jaar na de datum van inwerkingtreding van de overeenkomst een juridisch en technisch kader voor het extraheren van gegevens op het EU-grondgebied voor te leggen en uiterlijk drie jaar na de inwerkingtreding van de overeenkomst een voortgangsverslag in te dienen over de ontwikkeling van een soortgelijk EU-systeem[2]. Ook wordt in artikel 11 van de TFTP-overeenkomst tussen de EU en de VS bepaald dat de Commissie tijdens de geldigheidsduur van de overeenkomst een studie zal uitvoeren naar de mogelijke invoering

[1] PB L 195 van 27.7.2010, blz. 5.
[2] Besluit van de Raad van 13 juli 2010, PB L 195 van 27.7.2010, blz. 3.

van een soortgelijk EU-systeem, dat een meer gerichte doorgifte van gegevens mogelijk zou maken.

Ten behoeve van deze mededeling dient een dergelijk EU-systeem te worden onderscheiden van een kader voor gegevensextractie op EU-grondgebied. Onder *een kader voor gegevensextractie* op EU-grondgebied wordt een systeem verstaan waarmee de gegevens die de EU momenteel aan de VS verstrekt, op het grondgebied van de EU kunnen worden doorzocht. Daarentegen wordt onder *een soortgelijk EU-systeem* een onafhankelijk Europees systeem voor het traceren van terrorismefinanciering verstaan dat het mogelijk maakt de gegevens van de aangewezen verstrekker(s) in te zien, te doorzoeken en te analyseren. Voor de invoering van een EU-systeem is een wijziging van de TFTP-overeenkomst tussen de EU en de VS vereist.

1.2. Voorwerk

In december 2010 gaf de Commissie opdracht tot een *studie*, die in juli 2011 werd uitgebreid om ook de mogelijkheid van een regeling voor bewaring en extractie te onderzoeken. In het kader van dit onderzoek organiseerde de Commissie vier bijeenkomsten van deskundigen, waaraan werd deelgenomen door belanghebbenden als Europol, de Europese Toezichthouder voor gegevensbescherming, de aangewezen verstrekker van het TFTP[3] en vele deskundigen van de lidstaten die de betrokken ministeries, rechtshandhavingsinstanties, inlichtingendiensten en gegevensbeschermingsautoriteiten vertegenwoordigden.

Op 13 juli 2011 presenteerde de Commissie in haar *mededeling aan het Europees Parlement en de Raad (hierna "de mededeling van 2011" genoemd)* vijf opties voor een Europees systeem voor het traceren van terrorismefinanciering (hierna "EU-TFTS" genoemd). Hiervan werden er drie uitvoerbaar geacht. De mededeling van 2011 moest een discussie op gang brengen over de te volgen koers en een voorzet geven voor een effectbeoordeling.

De opties werden in oktober 2011 uiteengezet op de JBZ-Raad en in de commissie Burgerlijke Vrijheden, Justitie en Binnenlandse Zaken van het Europees Parlement.

Aangezien de lidstaten en het Europees Parlement geen duidelijke voorkeur uitspraken voor een bepaalde optie, werd besloten om alle opties in de effectbeoordeling van de Commissie te

[3] Society for Worldwide Interbank Financial Telecommunication (SWIFT)

onderzoeken en bovendien een aantal subopties uit te werken. Deze mededeling is gebaseerd op de effectbeoordeling[4].

2. DE BASISBEGINSELEN VAN DE COMMISSIE EN DE VASTGESTELDE OPTIES

2.1. Beginselen van de tijdens het Zweedse voorzitterschap vastgestelde informatiebeheerstrategie

In haar analyse van de voorgestelde koers houdt de Commissie rekening met de basisbeginselen van de informatiebeheerstrategie van 2009[5], die later zijn overgenomen en uitgebreid in twee mededelingen van de Commissie, waarvan de eerste een overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht betrof (2010)[6] en de tweede betrekking had op het Europees model voor informatie-uitwisseling (2012)[7].

Hierbij is het van het grootste belang dat de grondrechten en de beginselen van noodzakelijkheid, evenredigheid en kostenefficiëntie in acht worden genomen.

Het waarborgen van de *grondrechten* die zijn vastgelegd in het Handvest van de Grondrechten van de Europese Unie, in het bijzonder het recht op privacy- en gegevensbescherming, moet voor de Commissie voorop staan bij het formuleren van nieuwe voorstellen op het gebied van interne veiligheid die de verwerking van persoonsgegevens meebrengen. De artikelen 7 en 8 van het handvest stellen dat eenieder recht heeft op "eerbiediging van zijn privéleven [en] zijn familie- en gezinsleven" en op "bescherming van zijn persoonsgegevens". Artikel 16 van het Verdrag betreffende de werking van de Europese Unie, dat verbindend is voor de lidstaten, de instellingen en de organen van de Europese Unie, bevestigt het recht van eenieder op "bescherming van zijn persoonsgegevens". Volgens artikel 52 van het Handvest kunnen, met inachtneming van het evenredigheidsbeginsel, slechts beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

[4] SWD 2013 (xx) van
[5] Conclusies van de Raad over een strategie voor het beheer van rechtshandhavingsinformatie voor interne veiligheid in de EU, 16637/09.
[6] COM(2010) 385 van 20 juli 2010.
[7] COM(2012) 735 van 7 december 2012.

Beperking van het recht op privacy wordt *noodzakelijk* geacht als er sprake is van een dwingende behoefte, als de beperking evenredig is aan het nagestreefde doel en als de redenen die de overheid voor de beperking opgeeft, relevant en toereikend zijn.

Hoewel het moeilijk is om alle kosten van terrorisme in financiële termen uit te drukken, is het beginsel van *kostenefficiëntie* wel van toepassing. Een *kostenefficiënte* benadering houdt rekening met reeds bestaande systemen, om zo min mogelijk overlapping en zo veel mogelijk synergie te creëren. Er moet worden beoordeeld of de doelstellingen van een voorstel niet kunnen worden verwezenlijkt door bestaande instrumenten beter te gebruiken.

2.2. Aanpak

Gelet op de voornoemde beginselen heeft de Commissie onderzocht of een EU-TFTS noodzakelijk en evenredig met de kosten, de baten en de gevolgen voor de grondrechten is, in vergelijking tot de huidige situatie.

Wat de *baten* betreft, zou een EU-systeem de EU en haar lidstaten ruimere toegang tot relevante gegevens kunnen verschaffen en hun analytische capaciteiten om terroristen aan de hand van financiële transacties te traceren en te identificeren, kunnen vergroten. Aangezien financiële transacties waardevolle inlichtingen kunnen opleveren, die wellicht niet aan andere bronnen kunnen worden ontleend, vormen zij een instrument dat van groot belang zou zijn voor het opsporen van terroristische activiteiten en van de partijen die daarbij betrokken zijn. Een EU-TFTS zou dan ook kunnen worden gebruikt als een aanvullend inlichtingen- en onderzoeksinstrument voor het bestrijden van terrorisme en het verbeteren van de veiligheid in de EU; dit geldt des te meer als een dergelijk systeem meerdere verstrekkers van financiële gegevens en soorten transacties zou bestrijken. De baten van een EU-TFTS moeten worden afgezet tegen de geraamde kosten van het invoeren en onderhouden van een dergelijk systeem, met inbegrip van de financiële lasten voor de EU, de lidstaten en de aangewezen verstrekkers van de gegevens in kwestie.

2.3. Presentatie van de opties

Zowel voor *een kader voor gegevensextractie op EU-grondgebied* als voor *een soortgelijk EU-systeem* zijn meerdere opties overwogen.

2.3.1. Een kader voor gegevensextractie op EU-grondgebied

Een kader voor gegevensextractie op EU-grondgebied zou ten uitvoer kunnen worden gelegd met een door de aangewezen verstrekker beheerd systeem voor gegevensbewaring en -extractie, dat directe toegang tot gegevens biedt, zoals de VS thans op grond van het TFTP heeft. Deze directe toegang zou worden verschaft aan daartoe gemachtigde analisten of deskundigen van de VS.

Een van de mogelijkheden die deze optie biedt, bestaat erin gegevens gedurende een bepaalde tijd te bewaren op de server van de aangewezen verstrekker en zoekopdrachten direct op deze server uit te voeren. De huidige aangewezen verstrekker heeft overeenkomstig de TFTP-overeenkomst tussen de EU en de VS echter strenge maatregelen voor de bescherming en beveiliging van gegevens genomen, waardoor in de inhoud van berichten genoemde personen niet kunnen worden geïdentificeerd, wat tot gevolg heeft dat de huidige database niet aan de hand van persoonsgegevens kan worden doorzocht. Er zou dan ook een afzonderlijke database moeten worden opgezet.

Maar gegevens zouden ook kunnen worden geëxtraheerd en op een andere locatie in de EU bewaard. De tot het uitvoeren van zoekopdrachten gemachtigde analisten of deskundigen van de VS zouden ofwel fysiek kunnen worden ondergebracht in de gebouwen van de aangewezen verstrekker ofwel toegang op afstand tot de gegevens kunnen krijgen. Ongeacht de locatie van de gegevens zou in beide gevallen moeten worden gezorgd voor uitgebreide en solide waarborgen die aansluiten bij de specifieke kenmerken van het systeem.

2.3.2. Een soortgelijk EU-systeem

Er is een reeks opties voor een soortgelijk EU-systeem (als beschreven in de mededeling van 2011) onderzocht, waaronder een volledig gecentraliseerd systeem op EU-niveau, een gedecentraliseerd systeem op het niveau van de lidstaten en drie hybride systemen waarbij zowel de EU als de lidstaten een rol zouden spelen.

Elke optie biedt verschillende mogelijkheden voor het toepassingsgebied van het EU-systeem. Er moeten keuzes worden gemaakt met betrekking tot de soorten berichten en de aangewezen verstrekkers waarop het systeem betrekking zou hebben. Een soortgelijk EU-systeem zou beperkt kunnen blijven tot het soort financiële berichten en de aangewezen

verstrekker/aangewezen verstrekkers dat momenteel onder de TFTP-overeenkomst tussen de EU en de VS valt, maar ook verder kunnen reiken.

- De optie van een volledig gecentraliseerd systeem op EU-niveau houdt in dat één EU-orgaan alle belangrijke functies van het systeem verricht: het verzoekt om extractie van gegevens, slaat gegevens op, doorzoekt gegevens, analyseert inlichtingen, beveiligt en controleert het systeem en geeft nuttige inlichtingen door aan de lidstaten. Deze optie is juridisch onverantwoord, aangezien zij niet strookt met artikel 72 VWEU, dat bepaalt dat de verantwoordelijkheid voor de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid in de eerste plaats bij de lidstaten berust. Een dergelijk systeem zou voor de lidstaten niet uitvoerbaar, noch aanvaardbaar zijn, aangezien hiervoor op EU-niveau een soort gecentraliseerde inlichtingencapaciteit zou moeten worden opgezet.

- Een volledig gedecentraliseerd systeem op het niveau van de lidstaten houdt in dat het systeem door de bevoegde autoriteiten van de lidstaten wordt beheerd en dat er geen functies op EU-niveau worden vervuld. Dit betekent dat gegevens kunnen worden doorgegeven aan en doorzocht kunnen worden door alle 28 lidstaten tegelijk. Deze optie leidt tot meer gegevensstromen en brengt aanzienlijke kosten met zich mee. Ook wordt het risico van inconsistente behandeling van gegevens groter en ontstaan er ongelijke gegevensbeschermingsmechanismen. Daarom wordt deze beleidsoptie evenmin haalbaar geacht.

Deze twee opties zijn derhalve niet nader onderzocht.

Bij de drie overige opties voor een soortgelijk EU-systeem worden de verschillende functies verdeeld over verschillende organisaties op nationaal en EU-niveau.

Bij al deze hybride systemen moeten de gegevens telkens opnieuw worden aangevraagd bij de aangewezen verstrekker(s), en na extractie worden opgeslagen in een database op een veilige locatie in de EU. Voor de eigenlijke zoekopdrachten wordt vervolgens van deze centrale database gebruikgemaakt. Voor alle opties geldt dat moet worden voorzien in passende waarborgen inzake gegevensbescherming.

- A) Bij het eerste hybride systeem, de EU-TFTS-dienst voor coördinatie en analyse, moet een centrale EU-eenheid worden opgericht. Deze eenheid heeft als opdracht gegevens op te vragen bij de aangewezen verstrekker(s), zoekopdrachten uit te voeren, inlichtingen te analyseren en de resultaten te verspreiden. Anders dan bij een volledig gecentraliseerd systeem hebben de lidstaten directe toegang tot het systeem en kunnen zij de centrale eenheid of hun eigen analisten vragen om namens hen zoekopdrachten uit te voeren.

- B) Bij het tweede hybride systeem, de EU-TFTS-dienst voor gegevensextractie, moet eveneens een centrale EU-eenheid worden opgericht. In dit geval voert het EU-orgaan echter zoekopdrachten uit op verzoek van de lidstaten en verspreidt het resultaten onder de lidstaten zonder de inlichtingen te analyseren. Het EU-orgaan zou echter ook zelf zoekopdrachten mogen uitvoeren en de resultaten daarvan mogen analyseren.

- C) Bij het laatste hybride systeem, de dienst voor coördinatie van FIE's [8](financiële-inlichtingeneenheden), wordt een ad-hoc-EU-platform opgericht. Dit betreft geen permanent orgaan, maar een groep deskundigen op het gebied van financiële inlichtingen die voor vergaderingen bijeenkomt. Het FIE-platform kan wellicht voor dit doel worden versterkt. Elke lidstaat wijst één vertegenwoordiger aan die namens de lidstaat optreedt. Deze ad-hocautoriteit verzamelt de verzoeken van de FIE's van de lidstaten en verzoekt de aangewezen verstrekker(s) op grond van deze verzoeken van de lidstaten om gegevens. Elke vertegenwoordiger van een lidstaat is verantwoordelijk voor het uitvoeren van zoekopdrachten, het verrichten van analyses en het beheren van resultaten namens zijn eigen lidstaat. Vervolgens is het aan de bevoegde autoriteiten van de lidstaten om gebruik te maken van nuttige inlichtingen en deze op nationaal niveau te verspreiden.

2.3.3. Status-quo: TFTP-overeenkomst tussen de EU en de VS

Momenteel kunnen de EU en de lidstaten de VS vragen om zoekopdrachten uit te voeren op grond van de overeenkomst tussen de EU en de VS inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering (TFTP).

[8] Besluit 2000/642/JBZ van de Raad van 17 oktober 2000 inzake een regeling voor samenwerking tussen de financiële inlichtingeneenheden van de lidstaten bij de uitwisseling van gegevens.

Het TFTP is een instrument voor terrorismebestrijding dat de VS na de terreuraanslagen van 9/11 hebben ontwikkeld. Het is gebaseerd op het doorzoeken van de door de aangewezen verstrekker verstrekte gegevens, waaronder vanuit de EU doorgegeven gegevens.

In de TFTP-overeenkomst tussen de EU en de VS is nauwkeurig geregeld hoe de autoriteiten van de VS de gegevens moeten aanvragen. Europol controleert of de verzoeken om gegevens van de VS in overeenstemming zijn met de overeenkomst en met name of de verzoeken zorgvuldig op maat zijn gesneden, opdat zo weinig mogelijk gegevens worden doorgegeven. De overeenkomst bevat tal van bepalingen betreffende het veilig behandelen, bewaren en verwijderen van gegevens. Verstrekte gegevens worden in een beveiligde fysieke omgeving bewaard en gescheiden van andere gegevens opgeslagen. Krachtens de overeenkomst geldt een bewaringsperiode van vijf jaar en moet regelmatig worden beoordeeld of het nog nodig is de gegevens te bewaren. Twee van de in de VS gevestigde onafhankelijke toezichthouders zijn door de EU geselecteerd. Zij houden voortdurend toezicht op de manier waarop het systeem wordt beheerd en kunnen elke zoekopdracht van het U.S. Department of the Treasury controleren om zich ervan te vergewissen dat de zoekopdracht verband houdt met terrorisme of de financiering daarvan.

Ook bevat de overeenkomst bepalingen over het recht op toegang tot en rectificatie van persoonsgegevens, en bepalingen over beroepsprocedures. De overeenkomst bepaalt dat eenieder die van oordeel is dat zijn persoonsgegevens een met de overeenkomst strijdige verwerking hebben ondergaan, het recht heeft bij een administratieve of rechterlijke instantie beroep in te stellen, overeenkomstig respectievelijk het recht van de Europese Unie, van haar lidstaten of van de Verenigde Staten. De overeenkomst bepaalt dat eenieder, ongeacht nationaliteit of land van verblijf, de mogelijkheid heeft om volgens het VS-recht bij de rechter beroep in te stellen tegen een ongunstige overheidshandeling.

Tegen een ongunstige overheidshandeling van het Department of the Treasury in verband met krachtens de overeenkomst ontvangen persoonsgegevens kan onder meer beroep bij de rechter worden ingesteld op grond van de Administrative Procedure Act en de Freedom of Information Act. Op grond van de Administrative Procedure Act kunnen personen die schade hebben geleden door het optreden van de regering van de VS, beroep instellen bij de rechter. De grond van de Freedom of Information Act kunnen personen bij een administratieve of rechterlijke instantie beroep instellen om inzage te krijgen in overheidsdocumenten. De

bestaande uniforme procedures voor toegang tot en/of rectificatie, uitwissing of afscherming van persoonsgegevens, die door de Commissie, de VS en de Groep artikel 29 zijn overeengekomen, moeten het gemakkelijker maken voor EU-burgers om deze rechten uit te oefenen. De tenuitvoerlegging van de overeenkomst en de bijbehorende waarborgen en controles wordt overeenkomstig artikel 13 van de overeenkomst regelmatig geëvalueerd. Dergelijke evaluaties zijn in 2011[9] en 2012[10] verricht, en beide keren werd vastgesteld dat de overeenkomst correct ten uitvoer werd gelegd. Een derde evaluatie is gepland voor het voorjaar van 2014. Het ingevolge artikel 6 van de overeenkomst opgestelde gezamenlijk verslag over de waarde van de verstrekte gegevens beschrijft de baten van het TFTP wat betreft de preventie en bestrijding van terrorisme en de financiering daarvan. Ook wordt het gebruik dat meerdere lidstaten van het TFTP maken geboekstaafd. De nauwkeurige informatie uit het TFTP maakt het mogelijk om terroristen en de hen ondersteunende netwerken wereldwijd te identificeren en traceren. Hierdoor worden de financiële structuren van terroristische organisaties duidelijk en kunnen zowel nieuwe stromen van financiële ondersteuning als de betrokken actoren worden geïdentificeerd.

3. BEOORDELING

Bij de beoordeling of zij al dan niet zal voorstellen om een EU-TFST in te voeren, heeft de Commissie rekening te houden met uiteenlopende standpunten en verwachtingen inzake het ambitieniveau van een EU-systeem. Over de doelen van een EU-TFTS wordt door de diverse belanghebbenden en beslissers verschillend gedacht. De Commissie heeft de mogelijkheden en consequenties van beide scenario's getoetst aan de eerder uiteengezette beginselen die gelden voor de ontwikkeling en tenuitvoerlegging van nieuwe beleidsinitiatieven. Elke optie is met name geanalyseerd uit het oogpunt van noodzakelijkheid, evenredigheid en kostenefficiëntie.

3.1. Een kader voor gegevensextractie op EU-grondgebied

Zoals beschreven in punt 2.3.1 is de regeling inzake bewaring en extractie een optie waarbij de gegevens die momenteel in het kader van de TFTP-overeenkomst tussen de EU en de VS aan de VS worden doorgegeven, op het grondgebied van de EU worden verzameld, bewaard en doorzocht. Wat betreft inlichtingen levert het de EU of de lidstaten dus geen extra

[9] SEC(2011) 438 van 30 maart 2011.
[10] SWD(2012) 454 van 14 december 2012.

voordelen op ten opzichte van de huidige situatie. Wanneer de TFTP-gegevens in de VS en de EU worden bewaard, kan versnippering van de zoekopdrachten – die momenteel worden uitgevoerd op één verzameling TFTP-gegevens – zelfs ten koste gaan van de kwaliteit en de hoeveelheid nuttige inlichtingen en afbreuk doen aan de algehele efficiëntie van de TFTP. Het kan analyses ook aanzienlijk vertragen, aangezien het voor verder onderzoek van nuttige inlichtingen nodig kan zijn om verschillende achtereenvolgende zoekopdrachten uit te voeren op TFTP-gegevens op twee locaties. Bij terrorismeonderzoek is echter vaak snelheid geboden.

Dat gegevensextractie op Europees grondgebied plaatsvindt in plaats van in de VS, betekent niet automatisch dat persoonsgegevens beter worden beschermd. Ongeacht de locatie, is het voor een passende behandeling van gegevens van het grootste belang dat de toegang tot de gegevens beschermd is. Er moeten dan ook solide waarborgen komen om te verzekeren dat de gegevens in overeenstemming met de nodige voorschriften worden behandeld en verwerkt. Het systeem moet over een controlefunctie beschikken die de verzoeken om zoekopdrachten en de onderbouwing daarvan toetst. De onafhankelijke toezichthouders spelen een cruciale rol om te waarborgen dat de gegevens worden gebruikt voor de beperkte doeleinden die in de overeenkomst tot instelling van het kader worden bepaald. Er moeten maatregelen worden genomen om niet-geautoriseerde toegang tot of verstrekking van de gegevens te voorkomen, bijvoorbeeld door de gegevens in een beveiligde fysieke omgeving te bewaren. Ook moet er in procedures voor toegang tot en rectificatie van persoonsgegevens en in beroepsprocedures worden voorzien. Het is noodzakelijk een externe audit te laten verrichten om te waarborgen dat het systeem naar behoren functioneert.

Op grond van de TFTP-overeenkomst tussen de EU en de VS heeft de VS geen toegang tot alle gegevens van de aangewezen verstrekker, maar slechts tot groepen gegevens waarom de VS heeft verzocht en die Europol heeft goedgekeurd op basis van eerdere en actuele analyses van het terrorismerisico. Zonder een dergelijk mechanisme dat de reikwijdte van verzoeken om gegevens vanaf het begin beperkt, worden gegevens nog kwetsbaarder en de gevolgen uit het oogpunt van de gegevensbeschermingsrechten nog groter, als alle gegevens van de aangewezen verstrekker direct kunnen worden doorzocht. Dit betekent dat de wijze waarop de aangewezen verstrekker te werk gaat en zijn gegevens worden opgeslagen, aanzienlijk moet worden aangepast. De vorm waarin het onder de overeenkomst vallende financiële berichtenverkeer momenteel wordt bewaard, sluit identificatie van in de inhoud van berichten

genoemde personen uit. Elk financieel bericht wordt versleuteld en kan alleen worden opgezocht aan de hand van metagegevens zoals de verzenddatum, het soort bericht en de verzendende en ontvangende banken. De aangewezen verstrekker heeft voor strenge maatregelen voor de bescherming en beveiliging van gegevens gezorgd om de gegevens van zijn klanten wereldwijd te beschermen. Om het mogelijk te maken zoekopdrachten direct op de huidige server van de aangewezen verstrekker uit te voeren, moeten al deze berichten eerst worden ontsleuteld. Dit zou buitensporig en onevenredig zijn, aangezien de server van de aangewezen verstrekker meer berichten bevat dan alleen berichten die nodig zijn voor de bestrijding van terrorismefinanciering. Directe toegang met het oog op het uitvoeren van zoekopdrachten maakt bovendien een al te grote inbreuk op de dagelijkse activiteiten van de aangewezen verstrekker en leidt tot forse operationele, veiligheids- en systeemrisico's. Er moet dan ook een afzonderlijke database op EU-grondgebied worden opgezet waarin de nodige gegevens van de aangewezen verstrekker wordt bewaard.

Grote investeringen zijn geboden om het systeem in te voeren en te waarborgen dat het volledig aan de veiligheidsvoorwaarden voldoet. De gebouwen van de aangewezen verstrekker of een andere veilige locatie moeten aan de specifieke vereisten worden aangepast, er moeten technische en IT-oplossingen worden ontwikkeld en onderhouden, en voor het beheer van en het toezicht op het systeem moet gekwalificeerd personeel in dienst worden genomen en opgeleid.

Bij deze optie draaien de EU en de lidstaten op voor alle ongemakken en kosten van een mechanisme dat uitsluitend wordt opgezet ten behoeve van het TFTP, een instrument dat in handen is van een derde land. Vooralsnog lijkt deze optie niet noodzakelijk, evenredig of kostenefficiënt te zijn, aangezien zij geen extra voordelen op inlichtingengebied oplevert, kostbaar en lastig is om ten uitvoer te leggen en risico's voor de bescherming van persoonsgegevens kan opleveren.

3.2. Een soortgelijk EU-systeem

De mogelijkheid van een volledig gecentraliseerd EU-TFTS is niet nader onderzocht, omdat hiervoor geen rechtsgrondslag is en de kans klein is dat de lidstaten er mee zouden instemmen dat de EU een centrale rol zou spelen op een gebied dat onder de bevoegdheid van de lidstaten valt. Een volledig gedecentraliseerd systeem is buiten beschouwing gelaten omdat dit grote kosten en tal van gevolgen voor de rechten inzake gegevensbescherming zou meebrengen. De

drie hybride systemen die zijn onderzocht, verschillen wat betreft de mate waarin de lidstaten controle houden over de zoekopdrachten die zijzelf en het gecentraliseerd EU-orgaan uitvoeren.

Als het toepassingsgebied van het soortgelijke EU-systeem wordt uitgebreid met geautomatiseerde clearinginstellingen, e-geld en andere niet-financiële gegevens, dan is dat bevorderlijk voor het inlichtingenwerk: in dat geval kan de EU betalingen binnen de EU beter traceren en kan er een systeem komen dat toekomstbestendiger is dan een systeem dat alleen op FIN-berichten is ingesteld. Elke toevoeging van een aangewezen verstrekker vergroot echter het risico van inbreuken op de rechten inzake gegevensbescherming en vereist daarom een strikt pakket voorwaarden, waarborgen en controlemaatregelen. Hierdoor nemen ook de administratieve lasten voor de aangewezen verstrekkers toe. Het opzetten van een dergelijk complex en hoge organisatorische en technische eisen stellend systeem leidt door de toevoeging van meerdere gegevensverstrekkers en berichten ook tot een forse kostenstijging.

Uit deze analyse volgt dat een haalbaar EU-TFTS alleen op FIN-berichtenverkeer moet zijn gericht, aangezien de Commissie van mening is dat de voordelen die het gebruik van meerdere gegevenssoorten en verstrekkers oplevert, niet opwegen tegen de hoge kosten voor particuliere ondernemingen en de schadelijke gevolgen voor de rechten inzake privacy- en gegevensbescherming die een dergelijk systeem zou meebrengen. Als het EU-systeem betrekking heeft op dezelfde aangewezen verstrekker en hetzelfde berichtenverkeer als het TFTP, zijn de nuttige inlichtingen die het oplevert in kwalitatief en kwantitatief opzicht vergelijkbaar met die van het EU-VS TFTP. Ook de kwetsbaarheid van de gegevens is vergelijkbaar.

Zoals hierboven is uiteengezet, zijn er drie opties voor zo'n soortgelijk EU-systeem: A) de EU-TFTS-dienst voor coördinatie en analyse, B) de EU-TFTS-dienst voor coördinatie en analyse, en C) de dienst voor coördinatie van FIE's.

Optie A is waarschijnlijk bevorderlijk voor de preventie van terrorisme en de versterking van de veiligheid in de EU. Dat zowel teams van de EU als van de lidstaten zoekopdrachten uitvoeren en resultaten analyseren, draagt ertoe bij dat ten volle rekening wordt gehouden met de specifieke behoeften op inlichtingengebied van de EU en de lidstaten en dat het systeem gebruikt wordt voor dreigingen die specifiek zijn voor de EU. Deze verbetering is alleen

haalbaar als de lidstaten op de middellange tot lange termijn meer informatie en analyse willen en kunnen delen. Het is onduidelijk in hoeverre zij inderdaad meer informatie zullen aanleveren. Aangezien de lidstaten de VS uit hoofde van het TFTP nog steeds kunnen verzoeken om zoekopdrachten uit te voeren, kan dit systeem bovendien alleen dan een meer samenhangend EU-beeld opleveren, als de lidstaten tot aanzienlijke investeringen en samenwerking bereid zijn.

Optie B kan enige positieve gevolgen hebben voor het voorkomen van terrorisme en het verbeteren van de veiligheid in de EU. Het systeem kan sneller inspelen op EU-dreigingsanalyses, aangezien de zoekopdrachten in overeenstemming met de specifieke behoeften op inlichtingengebied van de lidstaten worden uitgevoerd. De rol van het gecentraliseerde EU-orgaan beperkt zich bij deze optie echter tot het uitvoeren van zoekopdrachten en het doorgeven van de betrokken gegevens aan de verzoekende lidstaat; het treedt in de eerste plaats als op als poortwachter. Dit houdt in dat er geen analyse op EU-niveau plaatsvindt en dat de mate waarin de lidstaten buiten het systeem om analyses uitwisselen, bepalend is voor het ontstaan van een samenhangend inlichtingenbeeld voor de EU. Dat het systeem niet kan waarborgen dat zoekopdrachten op gelijkvormige wijze worden gedefinieerd, vergroot het risico van foute positieven, hetgeen weer inbreuk maakt op het recht op privacy- en persoonsgegevensbescherming.

Optie C voorziet in specifieke behoeften op inlichtingengebied van de lidstaten en draagt dus ook enigermate bij tot het voorkomen van terrorisme en het verbeteren van de veiligheid. Aangezien de nationale FIE's verantwoordelijk zijn voor de zoekopdrachten en de analyses van hun lidstaten, kleven aan deze optie dezelfde nadelen als aan optie B: een duidelijk beeld kan alleen tot stand komen als de lidstaten buiten het systeem om nauwer samenwerken. Bovendien kan het lastiger worden om verbanden te zien en terrorismefinanciering op te sporen, doordat de FIE alleen op financiële inlichtingen is gespitst en deze informatie losstaat van het breder inlichtingenwerk. Bij deze optie speelt de EU overigens een zeer beperkte rol en wordt de capaciteit hoofdzakelijk op nationaal niveau versterkt.

Al deze opties stellen de EU, de lidstaten en de aangewezen verstrekker voor aanzienlijke kosten, waaronder die voor de ontwikkeling van IT-infrastructuur, beveiligde faciliteiten en tientallen, zo niet honderden werknemers voor het beheer van het systeem en de tenuitvoerlegging van waarborgen en controles. Elk van deze systemen kan de Europese

veiligheidssituatie bevorderen met behulp van dreigingsanalyses die voorzien in Europese behoeften.

Een onafhankelijk inlichtingen- en onderzoeksinstrument op Europees grondgebied maakt de doorgifte van gegevens aan de VS overbodig. Bij elk EU-TFTS blijven uitgebreide waarborgen en controles inzake gegevensbescherming nodig, zoals die momenteel op grond van de TFTP-overeenkomst tussen de EU en de VS van toepassing zijn; deze moeten in elk geval in overeenstemming zijn met het acquis inzake gegevensbescherming van de EU en de lidstaten. Voor elk verzoek om gegevens in EU-systemen te doorzoeken, moet worden gecontroleerd of het in overeenstemming is met het enige toegestane doel, namelijk de bestrijding van terrorisme en terrorismebestrijding, en of doorgifte van de betrokken gegevens gerechtvaardigd is. Gekwalificeerde onafhankelijke toezichthouders moeten zich ervan vergewissen dat elke zoekopdracht van de EU of een lidstaat naar behoren geautoriseerd is en noodzakelijk voor de bestrijding van terrorisme en terrorismefinanciering. De veilige behandeling en bewaring van gegevens moet worden gewaarborgd en niet-geautoriseerde toegang tot de gegevens moet worden voorkomen. De werking van het systeem en alle waarborgen moet aan een externe audit worden onderworpen. Alle nodige procedures voor toegang tot en rectificatie van persoonsgegevens en alle beroepsprocedures moeten in het systeem worden geïntegreerd.

Kortom, de Commissie heeft conform de verzoeken van het Europees Parlement en de Raad de mogelijke opties voor een EU-TFTS beoordeeld, waaronder een regeling inzake extractie en bewaring.

Bij deze beoordeling zijn de beginselen van de onder het Zweedse voorzitterschap vastgestelde informatiebeheerstrategie in aanmerking genomen. Een systeem moet hoe dan ook noodzakelijk, evenredig en kostenefficiënt zijn en in overeenstemming zijn met de grondrechten. De analyse van de Commissie, die in de onderhavige mededeling en de bijbehorende effectbeoordeling uiteen is gezet, wijst uit dat aan elk van de uitvoerbare opties voor- en nadelen verbonden zijn. Zoals uitgelegd, heeft de Commissie de niet-uitvoerbare opties buiten beschouwing gelaten.

Uit de verzamelde informatie blijkt niet duidelijk dat het op dit moment noodzakelijk is een voorstel voor een EU-TFTS te presenteren.

De Commissie ziet de mening van het Europees Parlement en de Raad over deze mededeling met belangstelling tegemoet.