KONINKRIJK BELGIE

COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

Brussel,

Adres : Hoogstraat, 139, B-1000 Brussel
Tel.: +32(0)2/213.85.40 E-mail : commission@privacycommission.be
Fax.: +32(0)2/213.85.65 http://www.privacycommission.be

ADVIES Nr 37 / 2006 van 27 september 2006

O. Ref. : 10 / A / 2006 / 035

BETREFT : Advies betreffende de doorgifte van persoonsgegevens door de CVBA SWIFT ingevolge de dwangbevelen van de UST (OFAC)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (“Richtlijn 95/46/EG”);

Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (“WVP”), inzonderheid op artikel 29 § 1;

Gelet op de adviesaanvraag van het College voor Inlichtingen en Veiligheid van 6 juli 2006, door de Commissie ontvangen op 19 juli 2006;

Gelet op de briefwisseling met SWIFT;

Gelet op het verslag van de Heer De Schutter;

Brengt op 27 september 2006 volgend advies uit :

A. INLEIDING

Op 19 juli 2006 ontving de Commissie van het College voor Inlichtingen en Veiligheid een verzoek om een advies uit te brengen over “de vraag of er in het kader van het dossier “SWIFT” sprake is van een schending van de Belgische wetgeving, meer specifiek van de WVP. De Commissie werd verzocht om eveneens het College in het bezit te stellen van alle elementen die van nut kunnen zijn bij het invullen van haar mandaat.

Op haar zitting van 5 juli 2006 had de Commissie reeds besloten ambtshalve een onderzoek te openen in dit dossier op basis van artikel 32 § 1 WVP[1], aangaande de verwerking van persoonsgegevens onder de verantwoordelijkheid van SWIFT, een coöperatieve vennootschap onder Belgisch recht, met hoofdzetel in België en met beperkte aansprakelijkheid (CVBA). Dit naar aanleiding van diverse persberichten die eind juni verschenen[2] over de rol van SWIFT bij de doorgifte van persoonsgegevens aan de US Department of the Treasury (UST), meer bepaald de Office of Foreign Assets Control (OFAC).

De Commissie nam tenslotte op 28 juni 2006 kennis van een publieke klacht die de organisatie “privacy International” formuleerde ten aanzien van de gegevensbeschermingsoverheden en –regulatoren van 33 landen in verband met voormelde persberichten.

Het onderzoek van de Commissie heeft zich exclusief toegespitst op de hoger vermelde problematiek en betrof dus niet de persoonsgegevensverwerkingen eigen aan de normale administratieve of managementsactiviteiten van een onderneming (personeelsadministratie, klantenbeheer, e.a.). De Commissie stelt in deze vast dat SWIFT daartoe bij de CBPL de nodige aangiften heeft verricht volgens de voorschriften van de WVP. De aandacht werd dan ook toegespitst op de gegevensstroom via de dienst “SWIFTNet FIN” en de mededeling aan de UST van de gegevens die via deze dienst worden gegenereerd. In verband met andere diensten heeft de Commissie geen kennis van transfer van gegevens aan de UST,

Voor het uitwerken van dit advies heeft de Commissie gesteund op SWIFT informatie die zich in de openbaarheid bevindt[3] , opgevraagde documentatie waar SWIFT inzage aan de Commissie toe verleende (toepassing van art. 31 § 1 WVP), elementen uit herhaalde bevragingen[4] en informatie bekomen tijdens overlegvergaderingen met SWIFT verantwoordelijken (algemeen adviseur of “general counsel”, de president-directeur of “CEO”, auditverantwoordelijke, juridische dienst, juridische raadgevers) op data van 23 augustus, 31 augustus (onderzoek ter plaatse) en tenslotte elementen uit de interne vergaderingen van de Commissie op 6 en 27 september 2006. Parallel daaraan werd ook een schriftelijke bevraging verricht bij de Nationale Bank van België via schrijven van 10 augustus 2006.
Vermelden wij tenslotte dat de problematiek van de doorgifte aan UST ook in behandeling is binnen de Europese Unie[5] en bij een aantal gegevensbeschermingsautoriteiten (“DPA’s”) in en buiten Europa (Duitsland, Italië, Frankrijk, Canada, Australië, e.a.).

---

[1] In een advies van 13 november 1996 betreffende het voorontwerp van wet tot aanpassing van de wet van 8 december 1992 aan de Richtlijn 95/46/EG, kan men lezen dat de Commissie zichzelf bevoegd beschouwt tot het uitvoeren van controles ter plaatse op eigen initiatief, of na een klacht of op grond van de aangifte van verwerkingen die zeer gevoelig zijn.

[2] Voornamelijk de New York Times (“bank Data is sifted by US in secret to block terror” van 22 juni 2006), (www.nytimes.com), de International Herald tribune (“oversight on records defended” van 25 juni 2006); , Los Angeles Times (“secret US Program tracks global bank transfers” van 23 juni 2006) en dooropvolgend wereldwijde persreacties.

[3] Voornamelijk de informatie op de website van SWIFT www.swift.com en andere gedrukte informatie

[4] Schrijven CBPL 7 juli en antwoord Swift 28 juli
Schrijven CBPL 8 september en antwoord Swift dd. 14 september 2006

[5] In de groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, opgericht op basis van artikel 29 van de richtlijn 95/46/EG, hierna de “Groep 29”.

De Commissie pleegde hierbij overleg met de Europese groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, opgericht op basis van artikel 29 van de richtlijn 95/46/EG (hierna de "Groep 29"). De Groep 29 verklaarde alvast op 26 september 2006[6] dat zij het als haar prioriteit beschouwt om de Europese dataprotectierechten te handhaven en wees ook op het gebrek aan transparantie van de onderhandelingen met de UST.

B. FEITEN EN JURIDISCHE CONTEXT

B.1. SWIFT

SWIFT is een coöperatieve vennootschap met beperkte aansprakelijkheid onder Belgisch recht, gevestigd in La Hulpe (België). SWIFT verleent aan haar klanten, zijnde financiële instellingen, geautomatiseerde, gestandaardiseerde diensten ("messaging services") en interface software met het oog op de transmissie van financiële boodschappen tussen financiële instellingen wereldwijd. SWIFT is dus zelf geen bank of andere vorm van financiële instelling.
Ongeveer 7.800 financiële instellingen zijn aangesloten bij SWIFT. In haar dienstverlening bezit SWIFT geen exclusiviteit. Financiële instellingen kunnen hun betalingsverkeer via andere aanbieders en middelen laten verlopen (VPN providers, internet, fax, netwerken van banken, VISA, etc. …). Naast verkoopskantoren in verscheidene landen, heeft SWIFT twee verwerkingscentra (OC), gevestigd in bijkantoren ("branches") van SWIFT, één in Europa en één in de Verenigde Staten. In deze OC worden, als onderdeel van de SWIFTNet FIN dienst, in spiegelbeeld, alle door SWIFT verwerkte berichten gedurende 124 dagen gestockeerd, teneinde in geval van betwistingen tussen financiële instellingen of verlies van gegevens voor een klant als "back-up recovery tool" te kunnen fungeren. Na die periode worden de gegevens gewist.

B.1.1. *Beschrijving van de gegevensstroom en gegevens die worden verwerkt via de SWIFTNet FIN dienst.*

De gegevensstroom die wordt verricht door SWIFT in het kader van de SWIFTNet FIN dienst betreft het sturen van boodschappen met betrekking tot financiële transacties tussen financiële instellingen. Er dient te worden opgemerkt dat SWIFT derhalve enkel contacten heeft met professionele klanten en geen directe contractuele relatie onderhoudt met klanten (natuurlijke personen) van financiële instellingen die een financiële transactie zouden aanvragen of ontvangen op of via hun rekeningen. SWIFT verleent haar diensten bovendien slechts aan financiële instellingen die een voorafgaand contractueel kader hebben ondertekend. Dit contractuele kader is gekend door de financiële instellingen die de SWIFTNet Fin dienst gebruiken en bestaat onder meer uit de SWIFT voorschriften ("by-laws"), de algemene voorwaarden, de specifieke documentatie in verband met de dienst (allen vermeld in het "SWIFT gebruikershandboek of "SWIFT User Handbook") en het SWIFT beleid inzake het ophalen van gegevens ("data retrieval policy").. Zij wordt aangevuld met het compliancebeleid[7] van SWIFT.

De elektronisch verstuurde boodschappen kunnen hierbij worden vergeleken met een "enveloppe" en een "brief", waarbij de "enveloppe" of het hoofd van de boodschap informatie betreft over de verzender, zijn BIC-code[8], een identificatie van de ontvangende bank en tenslotte de datum en het tijdstip van de boodschap. De "brief" (inhoud van de enveloppe), dus de eigenlijke boodschap, wordt hierbij geëncrypteerd via PKI encryptie en

[6] Zie de persverklaring gepubliceerd http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf
[7] De verklaring van SWIFT inzake compliance kan op haar website www.swift.com worden gevonden.
[8] BIC (Bank Identifier Code) is een internationale identificatiecode (ook wel eens swift-code genoemd), die toelaat elke individuele bank te herkennen.

bevat informatie die via gestandaardiseerde velden wordt ingevoegd. Indien het gaat om een boodschap in verband met een betaling van een klant van een bank[9] bevat deze informatie minstens het bedrag van de transactie, de munteenheid, de waardedatum, de naam van de begunstigde, de financiële instelling van de begunstigde, de klant die de financiële transactie verzocht en de financiële instelling van de klant die de transactie verzocht. Betalingsgerelateerde boodschappen kunnen evenwel ook andere informatie bevatten zoals referentienummers voor de betalingen en (voor sommige types boodschappen), "ongestructureerde tekst" ("free format").

Het traject van een internationale betalingsboodschap die via de SWIFTNet Fin dienst wordt gestuurd verloopt als volgt : (de eerste en vierde stap worden verricht buiten de werking van SWIFT)

1. een individuele betalingsopdracht van een opdrachtgevende klant (een individu of een onderneming) wordt gestuurd aan zijn bank (de "oorspronkelijke bank"). Tenzij de oorspronkelijke bank of de opdrachtgevende klant kiest voor een alternatieve dienst of oplossing naast SWIFT stelt de oorspronkelijke bank een gestandaardiseerde en geëncrypteerde SWIFT boodschap op;
2. de oorspronkelijke bank zendt de gestandaardiseerde SWIFT boodschap met gebruik van de SWIFTNet FIN dienst, of kiest een alternatief middel of oplossing naast SWIFT. Hierop wordt de boodschap hetzij aan een corresponderende bank het buitenland gestuurd, hetzij rechtsreeks aan de bank van de begunstigde (indien de oorspronkelijke bank een directe correspondentenrelatie heeft met de bank van de begunstigde);
3. de correspondentenbank zendt dezelfde boodschap door het SWIFT netwerk naar de bank van de begunstigde;
4. de bank van de begunstigde informeert de begunstigde dat zijn betaling is ontvangen en crediteert overeenkomstig de rekening van de begunstigde .

SWIFT handelt hierbij als de drager van de gestandaardiseerde boodschap in de gesloten enveloppe. De boodschappendienst omvat, op het niveau van de verwerkingscentra, een formele validatie van de inhoud ervan, met name naar de aanwezigheid of correcte inhoud van de data in de voorziene velden (bvb is de bank van bestemmeling ingevuld, is de munteenheid wel aangeduid, …). Dit vereist wel een ogenblik van decryptie van de inhoud van de boodschap, inclusief persoonsgegevens die geautomatiseerd verloopt. Als deel van de boodschappendienst worden de boodschappen ook bewaard in de verwerkingscentra in Europa en de VS voor voormelde periode van 124 dagen.

B.2. Dwangbevelen ("subpoenas")

Vanaf de aanslagen in september 2001 richtte de UST meerdere dwangbevelen aan het verwerkingscentrum van SWIFT in de VS. Na bevraging stelde SWIFT dat zij 64 dwangbevelen van de UST heeft ontvangen en nageleefd in de nasleep van de aanslagen van 11 september 2001 tot op heden.

[9] Een transfer door een klant is een van de negen categorieën van SWIFT boodschappen

Vóór 2001 was SWIFT ook reeds het voorwerp van enkele gerechtelijke of administratieve dwangbevelen, maar deze werden niet ingewilligd hetzij om termijnredenen (na 124 dagen) of omdat SWIFT kon aanvoeren dat de overheid de gegevens makkelijker kon verkrijgen van de zendende of ontvangende bank, of omdat SWIFT geen opzoekingsinstrument heeft in haar verwerkingscentra voor opvraging op naam OC. De dwangbevelen van de UST zijn van een totaal verschillend karakter en kunnen gekwalificeerd worden als ***niet geïndividualiseerde massale opvragingen ("Rasterfandung" of "carpetsweeping" techniek)*** in een eerste fase (zie infra). Het toepassingsgebied van de dwangbevelen is, zowel materieel, territoriaal als in de tijd zeer breed en wordt gedefinieerd in de dwangbevelen en in de onderhandelingsbriefwisseling tussen de UST en SWIFT.

De dwangbevelen werden toegepast voor alle transacties die verband of kunnen verband houden met terrorisme, in verband met een x-aantal landen en jurisdicties, op die datum, of van … tot … variërend van één tot meerdere weken, binnen en/of buiten de V.S., …). Het gaat dus zowel over boodschappen over interbancaire transacties binnen de V.S., naar of van de V.S., als van buiten de V.S., zoals bvb. binnen de EU.

Uit de meegedeelde informatie blijkt verder dat de UST in haar dwangbevelen uitgaat van een brede **definitie van "terrorisme"** als "de aanpak van aanvallen van terroristen tegen de VS die na 11 september 2001 plaatsvonden en een globaal netwerk van terroristencellen die een bedreiging zouden bieden voor verder geweld tegen VS onderdanen, VS eigendom en belangen en belangen in het thuisland en buitenland." Verder blijkt uit de onderhandelingen dat SWIFT met de UST een tweede (conventionele) definitie van terrorisme is overeengekomen, die luidt als volgt : "een activiteit die (i) een gewelddadige handeling inhoudt of een handeling die gevaarlijk is voor menselijk leven, eigendom, infrastructuur; en (ii) lijkt te beogen (A) een burgerlijke bevolking te intimideren of dwang uit te oefenen; (B) het beleid van een overheid te beïnvloeden door intimidatie of dwang; of (C) het gedrag van een overheid te beïnvloeden door massavernietiging, moord, kidnapping of het nemen van gijzelaars. Dit omvat, doch is niet beperkt tot, activiteiten die worden ontplooid door gekende organisaties van terroristen, maar sluit activiteiten uit van erkende overheden."[10] De Commissie merkt op dat in deze conventionele definitie de verwijzing naar de VS is weggelaten.

Uit de verificaties van de Commissie blijkt dat in het ophalingsproces een onderscheid **werd gemaakt tussen twee trappen**; enerzijds het bewaren van de onder de dwangbevelen aangeleverde boodschappen in een zwarte doos en anderzijds het effectief bekijken van boodschappen in de zwarte doos door de UST na uitoefening van zoekopdrachten. Beide stappen worden hierna beschreven.

Alle **boodschappen die onderworpen zijn aan de dwangbevelen** ("subpoened messages") worden geleverd door het verwerkingscentrum van SWIFT in de VS aan de UST en bewaard in een zogenaamde **zwarte doos** ("black box" of "production database") die wordt bewaard in faciliteiten van de UST.

In de zwarte doos vindt een automatische decryptering plaats met een tool (zoeksoftware) die werd ontwikkeld door de UST en de UST toebehoort, waarna de UST op naam opzoekingen kan doen. Deze zoeksoftware is niet beschikbaar voor SWIFT en verifieert of vooraf bepaalde namen van verdachten voorkomen in de boodschappen[11]. Er werd hierbij overeengekomen tussen SWIFT en de UST dat de UST alleen gerichte opvragingen mag verrichten die gerelateerd zijn aan punctuele onderzoeken naar terreuractiviteiten.

[10] "an activity that (i) involves a violent act or an act dangerous to human life, property, or infrastructure; and (ii) appears to be intended (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking. This includes, but is not limited to, activities engaged in by known terrorist organizations, but excludes activities of recognized governments."

[11] Zoals bevestigd door de UST aan SWIFT op 1 augustus 2002

SWIFT verschafte na formeel verzoek hiertoe door de Commissie geen precieze cijfers over het aantal boodschappen dat zich in de zwarte doos zou bevinden. Zij gaf hiertoe als reden dat deze informatie door de UST als van belang voor de nationale veiligheid werd geacht. Er werd ook medegedeeld dat deze informatie enkel door de UST kon worden vrijgegeven na toepassing van de gepaste veiligheidsprocedure voor Belgische ambtenaren met een passende veiligheidsmachtiging.

Desondanks kan men uit het algemene toepassingsgebied van de dwangbevelen en het gemiddelde volume van het aantal berichten dat dagelijks via de SWIFTNet FIN dienst wordt afgehandeld wel afleiden dat het aantal boodschappen dat is onderworpen aan de dwangbevelen en zich bevindt in de zwarte doos enorm hoog moet liggen. In een schrijven van 14 september 2006 bevestigde SWIFT dat de UST "het volle recht heeft onder Amerikaans recht om de SWIFT US afdeling te onderwerpen aan een dwangbevel teneinde **alle** SWIFT boodschappen mede te delen. Dit betekent dus dat, alleen al voor het jaar 2005, een totaal van 2.518.290.000 SWIFTNet Fin boodschappen aan dwangbevelen kan onderworpen worden[12].

B.3. Reactie van SWIFT op de dwangbevelen

SWIFT bekwam een aantal waarborgen en beschermingsmechanismen van de UST. De principes daarvan werden formeel gedocumenteerd in briefwisseling tussen SWIFT en de UST.

B.3.1. *Onderhandelingen met UST*

SWIFT besliste de dwangbevelen, uitgevaardigd tegen het SWIFT "bijkantoor" in de VS en niet tegen SWIFT CVBA, niet voor een Amerikaanse rechtbank aan te vechten, maar wel onmiddellijk met de UST te onderhandelen om duidelijk waarborgen te bekomen. SWIFT benadrukt dat zij in die continue onderhandelingen een uniek beschermingsniveau heeft bekomen voor de door haar overgemaakte data.

Voor zover de Commissie kon nagaan aan de hand van de voorgelegde documenten betroffen de eerste gedocumenteerde afspraken het aanstellen van een externe auditor (Booz, Allen & Hamilton") en de kenmerken van het auditproces met ingang van augustus 2002. SWIFT verkreeg op 15 september 2003 een "comfort letter" van de UST waarbij de UST haar steun betuigde aan SWIFT in geval derden zoals overheden van andere landen de naleving van de UST dwangbevelen in vraag zouden stellen. Met ingang van 14 april 2004 werden een aantal belangrijke waarborgen geïnventariseerd waarvan enkele waren onderhandeld van in het begin van het proces . Zij betroffen de conventionele vastlegging van de definitie van terrorisme en de criteria voor zoekopdrachten en ophalingen op 27 februari 2004, en afspraken omtrent de maximale vertrouwelijkheid van de opgehaalde data, de controle van SWIFT op de zoekcriteria en op de ophaling. Eveneens werd SWIFT de garantie gegeven dat de originele bron van de informatie (SWIFT) vertrouwelijk zou worden gehouden door de UST.

[12] Cijfer vermeld in hetzelfde schrijven van SWIFT van 14 september 2006. Men kan ook uitgaan van een gemiddeld en normaal dagelijks berichtenverkeer via SWIFTNet FIN dat tussen 6,9 miljoen (2005) en 11 miljoen berichten per dag (begin 2006) bedraagt en dat in zijn totaliteit aan de dwangbevelen kan onderworpen worden.

Samengevat betreffen de waarborgen, zoals overeengekomen tussen de UST en SWIFT :

- UST heeft geen toegang tot het SWIFT systeem zelf en de daarin opgeslagen gegevens;
- alleen gegevens in verband met onderzoeken naar terrorisme kunnen opgevraagd worden;
- de zoekopdrachten in de zwarte doos zijn alleen mogelijk op basis van specifieke, gerichte onderzoeksdossiers inzake terreuractiviteiten;
- een continue audit door de Amerikaanse auditor Booz, Allen & Hamilton werd voorzien vanaf medio 2002. Deze betreft end-to-end audits van het systeem van de UST teneinde SWIFT bijkomende waarborgen te verschaffen dat het systeem veilig was (conformiteit met ISO standaarden voor de beveiliging van informatie na te gaan), dat de doeleinden beperkt waren tot terrorismeonderzoeken, dat de scrutinizers (zie hierna) toegang hadden tot alle informatie waarrond de UST analisten onderzochten en teneinde continue verbeteringen aan het systeem aan te brengen;
- twee werknemers van SWIFT ("scrutinizers") kregen een veiligheidsmachtiging om aanwezig te zijn bij de extractie van de gegevens door de UST. Zij gaan de rechtvaardiging voor elke UST ophaling na op een reguliere basis initieel door statistische staalname ("statistical sampling"), later op 100 % niveau. Zij rapporteren enkel in verband met het respect van de extractieprincipes aan het management van SWIFT, niet op het detail van specifieke ophalingen;
- de UST zwarte doos blijft onderworpen aan de controle van de "scrutinizers" door middel van 24-uur toegang, real time monitoring en blokkeringmogelijkheid van de zoekopdrachten, zelfs vanaf het ogenblik dat de zwarte doos werd geplaatst op een fysiek beveiligde locatie van de Amerikaanse overheid;
- In het geval de UST een rechterlijk bevel zou zoeken om SWIFT te dwingen een dwangbevel na te leven, ging de UST akkoord om het naleven door SWIFT van de dwangbevelen niet te citeren als precedent of hierop te vertrouwen, waarbij SWIFT zich alle rechten van verdediging voorbehield in geval van zulke actie;
- de mogelijkheid werd voorzien voor SWIFT om van de UST alle niet-opgehaalde berichten uit de zwarte doos terug te halen, zij het onder de verplichting om deze data te bewaren voor zolang als de mogelijkheid bestaat dat een dwangbevel zou worden uitgevaardigd over deze data;
- strikte confidentialiteitsnormen zijn vastgelegd.

B.3.2. *Informatie aan de Toezichthouders*

Aanvankelijk werd enkel de juridische geldigheid van de dwangbevelen geverifieerd door de algemeen adviseur en externe adviseurs. Beslissingen over de naleving van de dwangbevelen werden genomen door de president-directeur (CEO) van SWIFT, het directiecomité ("Board of Directors"), en het auditcomité ("Audit and Finance Committee of "AFC"). Het directiecomité kreeg een korte toelichting over het dwangbevel door de voorzitter van het auditcomité. In maart 2002 werd aan het directiecomité een presentatie gegeven over dit onderwerp en werd een discussie over dit onderwerp gehouden. Periodiek wordt hierover verder gerapporteerd.

SWIFT bracht ook de "Senior level oversight Group" (G–10), waaronder de Nationale Bank van België op de hoogte. De Commissie bevroeg de Nationale Bank van België ("NBB") bij schrijven dd. 10 augustus 2006 in verband met de oversight bevoegdheden van de NBB. De NBB bevestigde in een antwoord van 29 augustus 2006 dat "de NBB in haar hoedanigheid van "overseer" in februari 2002 door SWIFT werd geïnformeerd over het bestaan van een Amerikaans dwangbevel gericht tegen het bijkantoor van SWIFT in de Verenigde Staten."

De NBB oordeelt niet bevoegd te zijn om de naleving door SWIFT van de opeenvolgende bevelschriften van UST te beoordelen. Dit standpunt wordt ook door de G-10 gedeeld.

C. TOEPASSELIJKHEID WVP

Nagegaan moet worden of de WVP toepasselijk is op SWIFT in haar hoedanigheid van uitbater van het SWIFTNet Fin systeem en dit als "verantwoordelijke voor de verwerking" of als "verwerker".

C.1. Territoriaal toepassingsgebied

De WVP is van toepassing *"op de verwerking van persoonsgegevens die wordt verricht in het kader van de effectieve en daadwerkelijke activiteiten van een vaste vestiging van de verantwoordelijke voor de verwerking op het Belgisch grondgebied (…)"* (artikel 3bis, 1° WVP).

De zetel en het hoofdkantoor van SWIFT zijn gevestigd in België en de vennootschap heeft een Belgisch ondernemingsnummer, zijnde 413330856. Het lijdt derhalve geen twijfel dat er sprake is van "*effectieve en daadwerkelijke activiteiten" en "een vaste vestiging" op het Belgisch grondgebied", los van de vraag of SWIFT de verantwoordelijke*[13] *voor deze verwerking is, een vraag die hierna zal worden behandeld*.

SWIFT verwees naar het feit dat het verwerkingscentrum in de VS geenszins een afzonderlijke rechtspersoonlijkheid heeft en dat er (binnen de normale interne verwerking van de dienst SWIFTNet FIN) geenszins sprake is van de mededeling van gegevens aan een externe vennootschap buiten de EU.

Vanuit vennootschapsrechtelijke hoek concludeert SWIFT op deze basis dat de verwerking steeds viel onder de regels waaraan de Belgische vennootschap onderworpen is, omdat dus het verwerkingscentrum juridisch zou kunnen worden geïdentificeerd met SWIFT SCRL. Zij leidt hieruit af dat de bescherming onder Belgisch recht ook van toepassing is op haar verwerkingscentrum in de VS. Hoewel SWIFT dit vennootschapsrechtelijk argument gebruikte teneinde de toepassing van artikelen 21 en 22 WVP in vraag te stellen (zie infra), merkt de Commissie op dat dit vennootschapsrechtelijke argument wel bijkomend kan bevestigen dat de verwerking van persoonsgegevens onderworpen is aan Belgisch recht, inclusief de WVP.

C.2. Materieel toepassingsgebied

Uit de beschrijving van de gegevensstroom en gegevens die worden verwerkt via de SWIFTNet Fin dienst (zie supra onder rubriek B.1.) blijkt duidelijk dat er sprake is van een "verwerking" van "persoonsgegevens" in de zin van artikel 1 §§1 en 2 WVP. De financiële boodschappen die worden verwerkt[14] en opgeslagen in het kader van de SWIFTNet FIN dienst bevatten immers gegevens van fysieke personen zoals de identiteit van de begunstigde en de identiteit van de opdrachtgever van financiële diensten zoals betalingsopdrachten.

Tenslotte kan worden opgemerkt dat artikel 10.10 van de algemene voorwaarden van SWIFT de toepasselijkheid van het Belgisch recht voorziet op de bepalingen en voorwaarden met betrekking tot het verstrekken van en het gebruik van de SWIFT diensten en producten. Hieronder dient uiteraard het Belgische recht inzake de bescherming van persoonsgegevens en de WVP te worden begrepen.

---

[13] Voor de analyse omtrent de verantwoordelijkheid van SWIFT, zie hierna.

[14] Volgens artikel 1 § 2 WVP is elke verzameling, opvraging, raadpleging, gebruik, verstrekking door middel van doorzending, verspreiding of op enigerlei andere wijze ter beschikking stellen van persoonsgegevens alsmede het elkaar in verband brengen van persoonsgegevens een verwerking.

D. BEOORDELING OF SWIFT, DE FINANCIËLE INSTELLINGEN EN DE NATIONALE BANK VAN BELGIË VERANTWOORDELIJKE VOOR DE VERWERKING OF VERWERKERS ZIJN

Bij het beantwoorden van de vraag van het College voor inlichtingen en veiligheid dient de rol te worden nagegaan van SWIFT, de klanten van SWIFT (hierna "financiële instellingen) en de Nationale Bank van België in het licht van de WVP.

De vraag is of SWIFT, de financiële instellingen of de nationale bank van België dienen gekwalificeerd te worden als verantwoordelijke voor de verwerking dan wel als verwerker. De verantwoordelijkheid tot naleving van de WVP wordt in beginsel opgelegd aan de verantwoordelijke voor de verwerking. Artikel 1 § 4 WVP definieert de verantwoordelijke voor de verwerking als *"(…) de rechtspersoon (…) die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt."* Verwerker is daarentegen de *"natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur (…) die ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt, met uitsluiting van de personen die onder rechtstreeks gezag van de verantwoordelijke voor de verwerking gemachtigd zijn om de gegevens te verwerken".* Het onderscheid tussen beide kwalificaties heeft zeer belangrijke gevolgen voor wat betreft de naleving van de WVP: de verwerker heeft in beginsel een beperktere verantwoordelijkheid onder de WVP en de betrokkenen kunnen hun rechten in beginsel enkel uitoefenen bij de verantwoordelijke.

De wettelijke definitie in artikel 1 § 4 WVP is **van dwingend recht** en hiervan kan niet bij contractuele afspraken worden afgeweken.

Bij de bepaling van wie verantwoordelijke is voorziet de WVP essentieel een **functioneel criterium**. De vraag is met andere woorden wie "vat" had op de verwerking van persoonsgegevens via haar dienst SWIFTNet Fin of wie de facto de cruciale beslissingen kon nemen aangaande het doel en de middelen van de verwerkingen. Formele criteria, zoals de contractuele omschrijving van de diensten of de hoedanigheid van de contractspartijen zijn hierbij nuttig maar a priori niet beslissend.

Voor een correcte beoordeling van een mogelijke kwalificatie van voormelde actoren dient ook voor ogen te worden gehouden welke doelstellingen en dus welke verwerkingen worden geviseerd. De Commissie acht het noodzakelijk om een onderscheid te maken tussen de volgende verwerkingen : enerzijds het verzorgen van de werking van de SWIFTnet FIN dienst en anderzijds het verrichten van internationale betalingsopdrachten met beroep op de SWIFTNet FIN dienst.

D.1. <u>De verwerking van persoonsgegevens in het kader van de SWIFTnet FIN dienst</u>

SWIFT stelde systematisch dat zij voor de boodschappendienst geen verantwoordelijke voor de verwerking is, doch slechts een verwerker. In de contacten met de Commissie steunde SWIFT hierbij op een aantal argumenten die als volgt kunnen worden samengevat:

- SWIFT vergelijkt zichzelf met deze van de aanbieder van een telecommunicatie- of elektronische postdienst waarvan normaliter wordt aangenomen dat deze geen verantwoordelijke voor een verwerking is doch slechts een verwerker[15];

[15] Overweging 47 van de richtlijn 95/46/EG stelt dat "wanneer een bericht dat persoonsgegevens bevat, wordt verzonden via een telecommunicatie- of elektronische postdienst waarvan het enige doel is dit soort berichten door te geven, het de persoon is van wie het bericht uitgaat, en niet degene die de dienst aanbiedt, die normaliter zal worden beschouwd als verantwoordelijk voor de verwerking van de in het bericht vervatte persoonsgegevens; dat evenwel de personen die deze diensten aanbieden normaliter zullen worden beschouwd als verantwoordelijk voor de verwerking van de aanvullende persoonsgegevens die noodzakelijk zijn voor de werking van de dienst;

- SWIFT stelt dat in de contractuele afspraken met de financiële instellingen[16] de kwalificatie van SWIFT als verwerker werd vastgelegd;
- SWIFT voert aan dat zij als verwerker een "normale manoeuvreermarge" heeft om de organisatie van haar dienst te bepalen, met name op het niveau van de technische en organisatorische maatregelen die nodig zijn om de verwerking uit te voeren;
- SWIFT stelt dat zij haar diensten aanbiedt in een "business- to business" omgeving, waarbij zij geen directe contacten noch contractuele relaties onderhoudt met de klanten van de financiële instellingen, waaronder natuurlijke personen;
- SWIFT stelt tenslotte dat zij geen zoekcapaciteit heeft uitgebouwd of ontwikkeld, teneinde te zoeken op persoonsgegevens die eventueel in de door haar afgehandelde boodschappen zouden vermeld staan.

Gelet op de functionele definiëring van de verantwoordelijke onder de WVP, acht de Commissie de **context binnen dewelke de verwerking wordt verricht** (deze van een coöperatieve vennootschap met beperkte aansprakelijkheid) en de **kennis van de exacte positie van de financiële instellingen en het bestuur van de CVBA SWIFT** cruciaal om een juiste kwalificatie te verrichten met betrekking tot de normale verwerking van gegevens binnen de SWIFTNet FIN dienst.

De vergelijking van de CVBA SWIFT met een normale aanbieder van een telecommunicatie- of elektronische postdienst is een formeel argument en lijkt ontoereikend. Deze formele vergelijking impliceert immers dat de CVBA SWIFT een vergelijkbare positie zou hebben met deze van elk willekeurig telecombedrijf dat op internationaal vlak een VPN kan aanbieden voor het uitwisselen van financiële boodschappen. In realiteit blijkt SWIFT evenwel een complexer werkingsmodel en dienstenmodel te hanteren dat uitgaat van een **internationaal coöperatief netwerk met een sterk centraal beheer** ten opzichte van de 7800 financiële instellingen die de dienst gebruiken. De uitbating en werkingsmodaliteiten van dergelijke netwerken verschillen fundamenteel van het eenvoudig dienstenconcept waarbij een enkele professionele aanbieder persoonsgegevens verwerkt ten aanzien van een professionele of niet-professionele tegenpartij. De beoordeling van de kwalificatie "verantwoordelijke" of "verwerker" is in deze context delicaat. Bij een cumulatie van de diverse actoren dienen de rol en verantwoordelijken van elke entiteit immers duidelijk te worden bepaald.

De normale verwerking binnen de SWIFTNet FIN dienst lijkt op het eerste zicht vrij ondoorzichtig door haar internationaal en non-transparant karakter. De structuur van (internationale) coöperatieve netwerken is evenwel niet uniek en kent twee duidelijke precedenten.

- Zo werd voor internationaal uitgebate negatieve lijsten van VISA en Mastercard-handelaren reeds door de Groep 29 aanvaard dat voor het uitbaten van coöperatieve internationale netwerken een medeverantwoordelijkheid van financiële instellingen en database operatoren (VISA, Mastercard) aangewezen lijkt[17]. De database operatoren hebben hierbij geen direct contact met de betrokken personen en zijn in principe enkel werkzaam in een "business to business" omgeving, hoewel hun diensten wel via hun contractspartijen in het "retail" circuit worden verdeeld.

[16] Zie Artikel 4.5.3 van de algemene voorwaarden van SWIFT die betrekking heeft op "verplichtingen inzake gegevensbescherming" ("Data Protection Obligations"). In haar contractuele documentatie maakt SWIFT een onderscheid tussen het verwerken van persoonsgegevens die verkregen zijn van de financiële instellingen bij het ondertekenen of het gebruik van de SWIFT diensten enerzijds en anderzijds de persoonsgegevens die in de boodschappen of bestanden door de financiële instellingen via de SWIFT diensten of producten worden verwerkt. Wat deze laatste verwerking betreft werd expliciet bepaald dat de financiële instellingen geacht worden verantwoordelijke voor de verwerking ("data controller") te zijn.

[17] Zie paragraaf 16 van de Guidelines for Terminated Merchant Databases van 11 janauri 2005 die stelt dat "The development and operation of a terminated merchant database require the joint action of two Participants acting as joint data controllers for any particular set of personal data relating to a specific merchant, namely 1) the Database Operator, and 2) the Participant that has a contractual relationship with the merchant."

- De piramidale structuur van de bestaande geautomatiseerde boekingssystemen (Computer Reservation System of "CRS") in de luchtvaartsector blijkt een tweede precedent. Hierbij voeren (onder meer) reisbureaus en luchtvaartmaatschappijen persoonsgegevens in de reservatiesystemen, de nationale distributieondernemingen bieden toegang op het reservatiesysteem aan tegen een vergoeding (reservatiegeld) en tenslotte wordt op het hoogste niveau het centraal beheer van het reservatiesysteem verzorgd. De Commissie[18] en de Franse gegevensbeschermingsautoriteit CNIL[19] verdedigden hier reeds het standpunt van de gezamenlijke verantwoordelijkheid.

De gegevensbeschermingsoverheden blijken dus voor voormelde coöperatieve netwerken de laatste jaren vooral uit te gaan van een medeverantwoordelijkheid van de professionele gebruikers van de database en de databasebeheerder.

Nu gewezen is op de context binnen dewelke de verwerking wordt verricht blijft het de vraag of en in welke mate SWIFT en/of de financiële instellingen het doel en de middelen van de SWIFTNet FIN dienst bepaalden. SWIFT is een medeverantwoordelijke, voor zover zij, met anderen (de financiële instellingen), te weten gezamenlijk, het doel en de middelen voor de verwerkingen bepaalt.

- De dienst van SWIFT is **geen zuivere transportdienst** en kan niet herleid worden tot de uitvoering van een opdracht voor iemand anders, die deze opdracht volledig zou bepalen. De realiteit is dat het bestuur van SWIFT, veeleer dan de financiële instellingen, de modaliteiten voor het leveren van de diensten bepaalt via **toetredingscontracten en technische standaarden die grotendeels vastliggen**. Overigens, indien elke individuele financiële instelling een bepaalde format of aanpassing van de gegevensbescherming zou wensen en kunnen implementeren, dan is het duidelijk dat de gestandaardiseerde verwerking van SWIFT in het gedrang zou kunnen komen. Het voorgaande belet echter niet dat, indien er een kritisch aantal vragen zou zijn (SWIFT sprak van een "vraag van de markt") tot aanpassing van de dienst of de ontwikkeling van een nieuwe dienst , SWIFT haar diensten aanpast in nauw overleg met haar leden. Een concreet voorbeeld van voormelde mogelijkheid ligt in het feit dat de informatie die wordt verwerkt in het kader van de SWIFTNet FIN dienst reeds werd aangepast na vraag van de Financial Action Task Force ("FATF") en consultatie van de financiële instellingen, teneinde de identificatiemogelijkheden van natuurlijke personen te verhogen[20].

- SWIFT is geen verwerker doordat zij beslissingen kan nemen aangaande het doel en de middelen van de verwerkingen, **beslissingen die overigens verder gaan dan de normale en wettelijk afgebakende "manoeuvreerruimte" binnen dewelke een normale verwerker kan beslissen** bij het uitoefenen van de aan hem toevertrouwde opdrachten. Doordat SWIFT, met de bewerkingen in het kader van de SWIFTnet FIN dienst eigen doeleinden nastreeft, is zij juist in staat om een toegevoegde waarde te bieden ten opzichte van de dienst verleend door haar concurrenten, waaronder haar eigen klanten. Een illustratie van de toegevoegde waarde die wordt aangeboden door SWIFT betreft de **automatische decryptie van de data in de verwerkingscentra waarbij SWIFT een formele verificatie verricht over de inhoud van elke boodschap**, teneinde de correcte inhoud van de voorziene velden na te gaan. Verder beslist enkel het bestuur van SWIFT over de plaatsing van de verwerkingscentra en de

[18] Zie de aanbeveling nr. 01/98 van de Commissie inzake het "Geautomatiseerde boekingssysteem" dd. 14 december 1998.

[19] De Commissie wijst hier op het voorbeeld van de geautomatiseerde reservatiesystemen die bestaan in de sector van de luchtvaart en die enerzijds klanten omvatten zoals de luchtvaartmaatschappijen en de reisbureaus en anderzijds de uitbaters van deze reservatiesystemen zoals Galileo. De verantwoordelijkheden van beide actoren werd reeds op 11 september 1996, ter gelegenheid van de 18° internationale conferentie aangaande de bescherming van privacy en persoonsgegevens toegelicht namens de CNIL. Zie de tekst op de site van de Canadese DPA : http://www.privcom.gc.ca/speech/archive/02_05_a_960918_03_f.asp

[20] Blijkens verslag

distributie van de diensten via de vestiging van haar verkoopskantoren. SWIFT blijkt tenslotte over een verregaande autonomie te beschikken bij het opleggen van haar gegevensbeschermingsbeleid aan de financiële instellingen, omtrent **elementen die buiten de normale verplichtingen van een verwerker en een verwerkersovereenkomst vallen** (zie artikel 16 § 1 WVP). Bijvoorbeeld, de "compliance policy" ("no comment policy"), verschilt van het beleid van een aantal (Europese) klanten van SWIFT en de privacyclausules die zich in de diverse SWIFT toetredingscontracten voor de SWIFTNet FIN dienst bevinden. Voormelde voorbeelden hebben betrekking op de essentiële feitelijke en juridische aspecten van de verwerking, waarover enkel de verantwoordelijke zeggenschap heeft, en niet de verwerker.

- Het is **niet ongebruikelijk dat de verantwoordelijken voor de verwerking geen rechtstreeks contact hebben met de betrokkenen** en de WVP vereist dit element ook niet om te spreken van een verantwoordelijke. Anders geformuleerd : de toepassing van de WVP wordt geenszins uitgesloten in een "business to business" context. Concrete voorbeelden van dergelijke verantwoordelijken die geen rechtstreeks contact of contractuele relatie hebben met de betrokkene werden reeds hiervoor vermeld (VISA, Mastercard, en distributieondernemingen en Computer Reservation Systems of "CRS").

- Indien men tenslotte zou pretenderen dat enkel de 7800 financiële instellingen verantwoordelijk zouden zijn voor de verwerkingen van de persoonsgegevens via de SWIFTNet Fin dienst, dan zou dit tot gevolg hebben dat de rechtszoekende zou geconfronteerd worden met een dermate grote **verspreiding en juridische fractionering van de betrokken verantwoordelijken,** waardoor het hen de facto onmogelijk zou worden gemaakt de rechten uit te oefenen die zij ontlenen aan de WVP.

- SWIFT is tenslotte geen verwerker omdat **het niet aan de verwerker toekomt om, op eigen initiatief en zonder informatie aan en fiat van de verantwoordelijke gedurende (bijna) 5 jaar cruciale beslissingen te nemen aangaande de ontvangst van gegevens** door administraties zoals de UST. SWIFT nam echter duidelijk alle cruciale beslissingen over de mededeling van gegevens aan de UST, en deed dit zonder medeweten van haar 7800 klanten. Dit blijkt uit volgende elementen :

  1. De beslissende rol van SWIFT bij de mededeling van de gegevens aan de UST blijkt uit de continue en geheime onderhandelingen met de UST en de afspraken die in dit kader werden gemaakt vanaf eind 2001. De concrete toepassing van de dwangbevelen werd door SWIFT in het geheim onderhandeld door het opzetten van de "zwarte doos" constructie, en later gecontroleerd via de vastlegging van de zoek- en de ophalingscriteria, het auditproces en de scrutinizers (zie supra). SWIFT bekwam ook de garantie dat de informatie over de bron zou worden vertrouwelijk gehouden.

  2. Vanuit het Belgisch hoofdkantoor werden de cruciale beslissingen genomen en opgevolgd aangaande de mededeling van de gegevens aan de UST. Dit betrof de beslissing om de wettelijkheid van het Amerikaanse dwangbevel van oktober-november 2001 te onderzoeken en hiermee in te stemmen, de eerste beslissing om de doorgifte te verrichten die werd verricht in gezamenlijk overleg tussen de algemeen adviseur, de president-directeur en het hoofd van de audit en de delegatie door het directiecomité aan het auditcomité tot verificatie van het extractieproces. De 7800 klanten van SWIFT werden niet geïnformeerd over de geheime beslissingen van SWIFT die in overleg met de UST werden genomen.

  3. De klanten van SWIFT blijken zelfs niet geïnformeerd over de concrete omvang en modaliteiten van de overdracht van gegevens aan de UST. Deze aanpak steunt op

de “no comment policy” in het compliancebeleid[21] dat het bestuur van SWIFT sinds 1993 heeft vastgelegd.

4. In de nasleep van de persberichten van juni 2006 bleken de klanten van SWIFT tenslotte zelfs niet bij machte om de mededeling aan de UST te stoppen. Na de persberichten aangaande dwangbevelen verzocht een Oostenrijkse kredietinstelling[22] SWIFT om te stoppen met gegevens mede te delen aan de UST. SWIFT weigerde bij schrijven dd. 9 augustus 2006 in te gaan op het verzoek van haar klant, stellend dat haar US afdeling onderworpen is aan de jurisdictie van de VS en dat zij de dwangbevelen dient na te leven op voorwaarde dat deze geldig en afdwingbaar zijn onder Amerikaans recht.

Op basis van voormelde overwegingen concludeert de Commissie dat SWIFT een verantwoordelijke is in de zin van de WVP voor de verwerkingen die worden verricht via de dienst SWIFTNet FIN . Hierna wordt onderzocht of er ook sprake is van een mede-verantwoordelijkheid, voor zover SWIFT samen met de financiële instellingen het doel en de middelen voor de verwerkingen bepaalt.

D.2. <u>Het verrichten van internationale betalingsopdrachten met beroep op de SWIFTNet FIN dienst</u>

Het is verder de vraag of de financiële instellingen mede het doel en de middelen hebben bepaald van de verwerking, zodat zij medeverantwoordelijke zijn in de zin van de WVP

Opnieuw is het belangrijk om oog te hebben voor de context binnen dewelke de financiële instellingen persoonsgegevens meedelen aan SWIFT. **De financiële instellingen treden in beginsel op een ander niveau, zijnde het niveau van het afhandelen van de betalingsopdrachten**. Deze verwerking is verschillend van de uitwisseling van de *financiële boodschappen* die, op “business to business” (doorgaans interbancair) vlak, door SWIFT wordt verricht. De uitwisseling van financiële boodschappen heeft uiteraard wel praktisch verband met de betalingsopdrachten. De uitwisseling en dataopslag blijkt juist, *ingevolge de betalingsopdracht, noodzakelijk om de transactie correct en veilig af te handelen in het interbancaire verkeer*. De SWIFT verwerking speelt zich niet af “aan het loket”, in direct contact met de betrokkene die instructie geeft om een betalingsopdracht te verrichten. Zij wordt integendeel verricht in de “back office” context van de financiële instellingen waar toepassingen zoals het inscannen van de betalingsopdrachten en het uitvoeren van interbancaire opdrachten in beginsel worden verricht conform de professionele standaarden en gebruiken van elke financiële instelling, de gebruiken van de sector en de bestaande normen. De Commissie besluit dat de verwerkingen “verzorgen van betalingsopdrachten” en “uitwisselen van betalingsberichten” in de praktijk vaak aan elkaar zijn gekoppeld, doch dat het verschillende operaties betreffen waarvan de doelstellingen en dus verwerkingen niet kunnen worden gelijkgesteld.

SWIFT stelde dat de financiële instellingen verantwoordelijk zijn voor het verrichten van de verwerking die erin bestaat om internationale betaalopdrachten af te handelen. De financiële instellingen die beroep doen op de SWIFTNet Fin zijn voor deze verwerking inderdaad geen verwerkers van SWIFT , gezien zij op dit vlak geenszins voor rekening van SWIFT handelen.

Het is ook belangrijk voor ogen te houden dat de financiële instellingen autonoom zijn en op interbancair vlak hun eigen doeleinden kunnen nastreven. De Commissie stelt vast dat de financiële instellingen in het interbancaire verkeer vaak cruciale beslissingen nemen over de mededeling van persoonsgegevens aan SWIFT, vaak zonder medeweten van hun klanten. Dit blijkt uit volgende elementen :

[21] De verklaring van SWIFT inzake compliance kan op haar website www.swift.com worden gevonden.
[22] De Niederoesterreichische Landesbank – Hypothekenbank AG, Kremsergasse 20 te 3100 St.-Pölten, Oostenrijk

- De financiële instellingen **beslissen in het interbancaire verkeer vaak autonoom over de middelen die worden ingezet voor de afhandeling van een gegeven betalingsopdracht**. Zij hebben de keuzevrijheid om al dan niet de dienst van SWIFT te gebruiken voor het uitsturen van financiële boodschappen in verband met individuele transacties. Zij kunnen desnoods alternatieve of concurrerende diensten gebruiken of ontwikkelen bij het doorsturen van deze financiële boodschappen in het interbancair verkeer (e-mail, fax, telefoon,… aan correspondentenbank,…). Keuzes op dit vlak zullen de globale privacykenmerken bepalen die verband houden met de betalingsopdrachten die de financiële instelling afhandelt. Gezien de diversiteit van de diensten op interbancair vlak staat het de financiële instellingen vrij om zich, bij de keuze van de interbancaire dienst te laten leiden door elementen zoals het privacybeleid van de professionele aanbieder, naast de beveiliging van de informatie die uiteraard steeds vereist is. De financiële instellingen kunnen een sterk privacybeleid van een bepaalde aanbieder of een bepaalde oplossing zoals een VPN gebruiken als garantie, teneinde het vertrouwen van hun klanten en hun diensten maximaal te waarborgen.

- De financiële instellingen **kennen het contractuele kader van de SWIFTnet FIN dienst**. Uit de contractuele documentatie (Data Retrieval Policy[23]) en het beleid van SWIFT inzake compliance blijkt dat de klanten van SWIFT **op de hoogte waren van het algemeen principe om persoonsgegevens mede te delen ingevolge de aan hen of aan SWIFT geadresseerde dwangbevelen**. SWIFT voerde aan[24] dat het aantal dwangbevelen dat aan financiële instellingen werd geadresseerd in de duizenden of zelfs tienduizenden per jaar zou lopen. Het kan dus worden betwijfeld dat de financiële instellingen die actief zijn op de internationale betalingsmarkt onwetend zouden zijn over het algemeen principe van de dwangbevelen.

- De financiële instellingen dienen als professionele dienstverlener **de mogelijke implicaties en (privacy)risico's voor de betrokken klant te kunnen inschatten die zouden verband houden met de SWIFTnet FIN dienst**, dat zij onderschrijven als professionele dienstverlener. Hierbij is het belangrijk om na te gaan of het privacybeleid van de opdrachtgevende instelling duidelijke bepalingen over deze risico's bevat.

- Gelet op hun directe contact met de eigenlijke opdrachtgevers voor de betalingsinstructies spelen de financiële instellingen een **essentiële "loketrol".** De Commissie sluit niet uit dat de financiële instellingen als "tussenpersoon" worden beschouwd voor het uitoefenen van de rechten van de betrokkenen in het kader van de SWIFTNet Fin dienst, voor zover dit gebeurt in duidelijke afspraak met SWIFT als verantwoordelijke voor de verwerking in het kader van de SWIFTNet Fin dienst.

Gelet op voormelde overwegingen is de Commissie van oordeel dat de financiële instellingen die actief zijn in het internationaal betalingsverkeer op "business to business" (interbancair) vlak mede het doel en de middelen kunnen bepalen van de hen toevertrouwde verwerkingen (de afhandeling van de betalingsopdrachten van hun klanten). In de mate dat gebruik wordt gemaakt van de dienst SWIFTNet Fin kunnen zij, samen met SWIFT, geacht worden medeverantwoordelijke voor de verwerking te zijn.

[23] Waar is bepaald "Teneinde elke twijfel uit te sluiten, zal niets in dit beleidsdocument of, meer algemeen, de vertouwelijkheidsplichten van SWIFT ten opzichte van haar klanten, worden beschouwd als een belemmering voor SWIFT om verkeersgegevens of gegevens uit boodschappen op te vragen, te gebruiken of mede te delen, voor zover redelijkerwijs noodzakelijk teneinde een goeder trouw dwangbevel of andere wettige procedure door een rechtbank of een andere bevoegde overheid na te leven ("For the avoidance of any doubt, nothing in this policy or, more generally, SWIFT's obligations of confidence to customers, shall be construed as preventing SWIFT from retrieving, using, or disclosing traffic or message data as reasonably necessary to comply with a bona fide subpoena or other lawful process by a court or other competent authority.")

[24] in reactie op een rapport van een vergadering met de Commissie dd. 22 augustus 2006

D.3. Verantwoordelijkheid van de National Bank van België

Bij gezamenlijke ontwerpresolutie van 5 juli 2006 uitte het Europees Parlement de wens ten aanzien van de lidstaten[25] om *"ervoor zorgen en zich ervan vergewissen dat er nationaal geen juridische leemte bestaat en dat de communautaire wetgeving inzake gegevensbescherming ook van toepassing is op de centrale banken".* De lidstaten werden derhalve gevraagd om de resultaten van deze verificatie over te maken aan de Europese Commissie, de Raad en het Europees Parlement.

De Commissie stelt vast dat de NBB als overseer noch het doel noch de middelen bepaalde van de verwerking van persoonsgegevens via de SWIFTNet Fin dienst. De NBB kan derhalve geen verantwoordelijke zijn in de zin van de WVP met betrekking tot voormelde verwerking. De NBB werd wel als overseer in februari 2002 door SWIFT geinformeerd over het bestaan van een Amerikaans dwangbevel.

Gelet op voormelde ontwerpresolutie wenste de Commissie bij de NBB als overseer na te gaan wat de concrete inhoud is van de "oversight", en in welke mate de NBB het als overseer als haar taak beschouwt om ervoor te waken dat SWIFT juridische risico's zoals privacyrisico's afdoende zou hebben afgedekt. De NBB antwoordde bij schrijven van 28 augustus 2006 dat
"(…) Krachtens artikel 8 van haar Organieke Wet[26] waakt de NBB over de goede werking van de verrekenings- en betalingssystemen. Deze opdracht sluit aan bij de taken van het Europees Stelsel van Centrale Banken (ESCB), inzonderheid artikel 22 van de statuten van het ESCB. Deze zeer specifieke opdracht van de centrale banken is bekend onder de benaming 'oversight'. Deze activiteit wordt uitgeoefend vanuit een systeemperspectief, waarbij de goede werking van het globale betalings- of verrekeningssysteem centraal staat teneinde de financiële stabiliteit te verzekeren en zogeheten "systeemrisico's" met een domino-effect van bankfaillissementen te vermijden.(…)" Verder werd geantwoord dat
"De Bank (…) vanuit haar hoedanigheid van overseer geen enkele verantwoordelijkheid bezit voor de handelingen van SWIFT. De goedkeuring of afkeuring van operationele, financiële, juridische of vennootschapsrechtelijke beslissingen van bedrijfsvoering wordt door SWIFT niet gevraagd aan de Bank noch verkregen ." en "*(…) dat de G-10 centrale banken in de loop van 2002 overleg pleegden inzake de aangelegenheid van de Amerikaanse bevelschriften en tot het besluit kwamen dat deze bevelschriften buiten het bereik vielen van het oversight van de centrale banken. Er werden nadien geen nieuwe elementen aangereikt die de Senior Level Oversight Group ertoe noopten dat besluit te herzien."*

Uit voorgaande elementen blijkt dat de naleving van de WVP door SWIFT vooralsnog niet als een onderdeel van het individueel of coöperatief oversight wordt beschouwd.

In de mate de NBB evenwel optreedt *als klant van SWIFT* en zij hierbij persoonsgegevens zou toevertrouwen aan de dienst SWIFTnet Fin, kan zij wel als verantwoordelijke worden beschouwd zoals vermeld onder rubriek D.2.

E. ONDERZOEK VAN MOGELIJKE SCHENDINGEN VAN DE WVP

Het verzoek om advies betreft de vraag naar mogelijke schendingen op de WVP door SWIFT.
De vraag of de (Belgische) financiële instellingen inbreuk pleegden op de WVP valt hierbij strikt genomen buiten het voorwerp van advies en kon binnen de beperkte tijd waarover de Commissie beschikte niet worden onderzocht. Gelet op het feit dat de Commissie evenwel

[25] Gezamenlijke ontwerpresolutie over het onderscheppen door de Amerikaanse geheime diensten van bankoverschrijvingsgegevens van het SWIFT-systeem
[26] Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de nationale bank van België

van oordeel is dat er sprake blijkt te zijn van medeverantwoordelijkheid in hoofde van de financiële instellingen, houdt de Commissie zich verder ter beschikking voor het beoordelen van eventuele inbreuken door individuele (Belgische) financiële instellingen.

De Commissie benadrukt dat er fundamentele verschillen bestaan tussen de EU en VS wat betreft de wetgevingen en beginselen die de verwerkingen van persoonsgegevens reglementeren. Verwerkingen van persoonsgegevens onder het Europees recht worden gekenmerkt door het hoge beschermingsniveau dat in Europa werd ingesteld krachtens de toepasselijke verdragen zoals artikel 8 EVRM, het Verdrag nr. 108[27] en de toepasselijke Europese Richtlijnen zoals de richtlijn 95/46/EG.

De Commissie wijst op **een aantal - vaak voorkomende – misverstanden die soms bestaan over de begrippen "passende bescherming" en "naleving van de norm of (privacy)wet".** Zij benadrukt dat bij de interpretatie van deze noties **het niet volstaat om enkel controle door een externe auditor te verrichten, technische standaarden of normen (bijvoorbeeld ISO) na te leven en te voorzien in een passende technische beveiligingsmaatregelen**. De toepasselijke beginselen onder de WVP rijken veel verder.

Hierna wordt dus nagegaan of SWIFT alle toepasselijke beginselen van de WVP heeft nageleefd, zelfs indien zij reeds een hoog niveau van beveiliging van gegevens zouden hebben bekomen. Bij de evaluatie werd een onderscheid gemaakt tussen de vraag of er enerzijds inbreuken op de WVP werden gepleegd in het kader van de normale werking van de SWIFTNet FINdienst en of er anderzijds inbreuken werden gepleegd op de WVP in het kader van de transfer van de gegevens aan de UST.

E.1. <u>Pleegde SWIFT inbreuken op de WVP in het kader van de normale werking van de SWIFTNet FIN dienst ?</u>

E.1.1. *Wettelijke basis (artikel 5 b) WVP en artikel 7 b) richtlijn 95/46/EG)*

Op basis van artikel 5 WVP kunnen de persoonsgegevens van de opdrachtgevers of begunstigden slechts in een limitatief aantal gevallen worden verwerkt. De verwerking van persoonsgegevens in het kader van de normale werking van de SWIFTNet FIN dienst lijkt legitiem voor zoverre zij noodzakelijk is voor de uitvoering van de overeenkomst tussen SWIFT en de betrokken kredietinstelling (artikel 5 b) WVP en artikel 7 b) richtlijn 95/46/EG).

E.1.2. *Informatieplicht (artikel 9 WVP en artikel 11 richtlijn 95/46/EG)*

In de mate SWIFT verantwoordelijke voor de verwerking is, is zij eveneens onderworpen aan de informatieplicht. Dit betekent onder meer dat de natuurlijke personen wiens gegevens in de betalingsboodschappen werden uitgewisseld minstens dienden op de hoogte te worden gebracht conform artikel 9 WVP. De betrokken personen dienden bijvoorbeeld te weten wie de ontvangers van de gegevens konden zijn die zij aan hun kredietinstelling overmaakten (SWIFT, overheden,..), en voor welke doelstellingen hun gegevens konden worden verwerkt.

Gezien SWIFT de persoonsgegevens verzamelt aan de hand van de opdrachten van de financiële instellingen verkrijgt zij de persoonsgegevens niet rechtstreeks van de betrokken personen. In dat geval dient volgens artikel 9 § 2 WVP (artikel 11 richtlijn 95/46/EG) "op het moment van de registratie van de gegevens of wanneer mededeling van de gegevens aan een derde wordt overwogen, uiterlijk op het moment van de eerste mededeling van de

[27] Verdrag van 28 januari 1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, B.S., 30 december 1993, goedgekeurd bij wet van 17 juni 1991 houdende goedkeuring van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981.

gegevens, de informatie[28] te worden verstrekt, *tenzij de betrokkene daarvan reeds op de hoogte zou zijn gebracht door de financiële instellingen".* Dit betekent dat, indien SWIFT er niet over gewaakt heeft dat de financiële instellingen de betrokkenen informeerden conform artikel 9 § 1 WVP en er geen specifieke uitzonderingsbepaling voorzien is op de informatieplicht in het uitvoeringsbesluit van de WVP, SWIFT een inbreuk pleegde op artikel 9 § 2 WVP.

Het feit dat SWIFT geen directe relatie onderhoudt met de betrokkenen kan tenslotte geenszins worden beschouwd als een afdoende reden om de informatieplicht niet na te leven, bijvoorbeeld via de financiële instellingen. Hoewel de WVP niet de concrete wijze voorschrijft waarop de informatie moet worden gegeven, kan rekening worden gehouden met de context waarin de gegevens worden verwerkt, op voorwaarde dat de gekozen informatietechniek tot doel heeft de betrokkenen effectief en duidelijk te informeren. De Commissie oordeelde reeds in het kader van het advies 48/2003 van 18 december 2003 met betrekking tot de overdracht van persoonsgegevens aan de Verenigde Staten door sommige luchtvaartmaatschappijen dat "de wijze waarop de informatie wordt medegedeeld aan de klant daarenboven onvoldoende uitdrukkelijk (is), gezien deze informatie verwerkt zit in de tekst betreffende de algemene vervoersvoorwaarden en medegedeeld wordt op aanvraag of via het Internet". Wel werd in een context van massamanifestaties zoals voetbalwedstrijden geoordeeld door de Commissie[29] dat de informatie individueel (op de toegangstickets) of collectief kon gebeuren (bv. door het aanbrengen van duidelijke en zichtbare borden aan de ingang van het stadion).

Gelet op haar medeverantwoordelijkheid in het licht van de WVP heeft SWIFT onvoldoende overleg gepleegd met de financiële instellingen teneinde de informatieplicht (artikel 9 WVP) na te leven. Dit heeft geleid tot onvoldoende informatie ten aanzien van de betrokkenen en de niet-naleving van artikel 9 WVP.

E.1.3. *Aangifteplicht (artikel 17 WVP en artikel 21 richtlijn 95/46/EG)*

Gezien SWIFT verantwoordelijke voor de verwerking is, is zij in principe onderworpen aan de toepassing van de aangifteplicht die een algemene, zij het minimale transparantie en controle mogelijk maakt. De Commissie stelt echter vast dat SWIFT geen aangifte verrichte voor de verwerking van persoonsgegevens in het kader van de SWIFTNet FIN dienst, in tegenstelling tot andere verwerkingen zoals de eigen personeelsadministratie van SWIFT die buiten het kader van dit advies vallen.

De Commissie is derhalve van oordeel dat **artikel 17 WVP niet werd nageleefd.**

E.1.4. *Doorgifte van persoonsgegevens naar een land zonder passend beschermingsniveau (artikelen 21 en 22 WVP en artikelen 25 en 26 richtlijn 95/46/EG)*

SWIFT diende rekening te houden met de reglementering op de doorgifte van persoonsgegevens naar derde landen. De bepalingen van de richtlijn 95/46/EG (hoofdstuk IV, in de artikelen 25 en 26) regelen deze problematiek en werden gedeeltelijk overgenomen in de WVP, meer bepaald in de artikelen 21 en 22 van de WVP.

SWIFT deelde de Commissie mee dat zij van oordeel is dat de vereiste van een passend beschermingsniveau onder artikel 21 WVP niet van toepassing zou zijn voor de verwerking

[28] Volgens artikel 9 § 2 WVP is de relevante informatie de *naam en adres van de verantwoordelijke, de doeleinden van de verwerking (…),* en *andere bijkomende informatie, met name de betrokken gegevenscategorieën en de ontvangers of de categorieën ontvangers, het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem betrekking hebben; behalve indien die verdere informatie, met inachtneming van de specifieke omstandigheden waaronder de gegevens verwerkt worden, niet nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen;*

[29] Advies 10/2005 van 15 juni 2005.

in het kader van haar SWIFTNet Fin dienst. Samengevat haalt zij hiervoor volgende argumenten aan :

- Het verbod van doorgifte van gegevens (artikel 21 § 1) zou niet gelden nu de doorgifte niet vanuit België werd verricht door de moedervennootschap.
- Het verbod van doorgifte van gegevens zou niet gelden nu de doorgifte niet werd verricht aan een derde vennootschap en nu volgens een vennootschapsrechtelijke regel het bijhuis (verwerkingscentrum in de VS) van SWIFT zonder rechtspersoonlijkheid juridisch gesproken steeds onder de moedervennootschap zou vallen. Deze juridische eenheid zou voor gevolg hebben dat de verwerking in het kader van de dienst SWIFTNet FIN steeds onderworpen blijft aan een passend beschermingsniveau, zijnde het Belgische recht.
- Subsidiair, voor zover de wettelijke uitzonderingen in artikel 22 § 1 WVP wel zouden van toepassing zijn, voert SWIFT aan dat de doorgifte noodzakelijk zou zijn voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, (artikel 22,2° WVP), hetzij dat de doorgifte noodzakelijk zou zijn voor de uitvoering van een overeenkomst in het belang van de betrokkene (artikel 22, 3° WVP), hetzij dat de doorgifte noodzakelijk zou zijn of wettelijk verplicht vanwege een zwaarwegend algemeen belang. (artikel 22, 4° WVP).
- De doorgifte gebeurt in een zeer sterk beveiligde omgeving en met encryptie van de inhoud van de boodschappen.

De artikelen 21 en 22 WVP zijn van toepassing van zodra er sprake is van het onderwerpen van persoonsgegevens aan een verwerking na een doorgifte van persoonsgegevens naar een land zonder passend beschermingsniveau zoals de VS. Opnieuw hanteert de WVP hierbij een **functioneel criterium**. Gelet op het feit dat de artikelen 21 en 22 WVP functioneel zijn omschreven en dwingend recht van openbare orde uitmaken, kunnen vennootschapsrechtelijke regels bezwaarlijk het ganse beschermingsregime krachtens de richtlijn 95/46/EG terzijde schuiven.

De Commissie stelt vast dat er, in het kader van de normale werking van de SWIFTNet FIN dienst, sprake is van een doorgifte van Europese berichten naar de verwerkingscentra in Europa én de VS. Het feit dat de gegevens aan een filiaal worden gestuurd is geen criterium volgens de privacywet om de voorwaarden van de wet niet toe te passen.

Deze transfer gebeurt dagelijks en massaal (11 miljoen berichten per dag begin 2006). Na doorgifte aan de verwerkingscentra worden de gegevens onderworpen aan het geheel van bewerkingen[30] die eigen zijn aan de SWIFTNet Fin dienst.

De Commissie merkt op dat het feit van verregaande beveiliging of encryptie van persoonsgegevens niet belet dat de transfer van gecodeerde gegevens nog steeds onderworpen is aan de artikelen 21 en 22 WVP.

De Commissie is verder van oordeel dat de uitzonderingen die worden voorzien in artikel 22 WVP niet van toepassing zijn op de verwerking via de dienst SWIFTNet FIN. Gelet op de alternatieven en concurrerende diensten die voorhanden zijn in de internationale betalingsmarkt kan een beroep op de dienst SWIFTNet Fin bezwaarlijk steeds noodzakelijk worden geacht voor elke financiële instelling om een betalingsopdracht uit te voeren.

Tenslotte dient de notie van “zwaarwegend algemeen belang” steeds onder de Belgische rechtsorde te worden ingevuld, conform de in België geldende rechtsnormen zoals artikel 8 EVRM. SWIFT voerde aan dat de plaatsing in spiegelbeeld van de verwerkingscentra beschouwd wordt als een kritisch element voor het mondiale financiële systeem. Zij stelt dat de plaatsing in spiegelbeeld haar werd opgelegd door de overseers (G-10 centrale banken) voor redenen van veiligheid en betrouwbaarheid, gezien de SWIFT infrastructuur

[30] Met name de automatische decryptie en formele verificatie van de data

als kritisch wordt beschouwd voor de globale financiële industrie. Op Europees vlak werd echter reeds geoordeeld dat de VS geen passend beschermingsniveau aanbiedt in het licht van de richtlijn 95/46/EG. Zelfs indien het mondiale financiële systeem ook de openbare orde in België zou raken, is dit echter geen afdoende rechtvaardiging in het licht van de richtlijn 95/46/EG om een verwerkingscentrum in de VS te plaatsen zonder passend beschermingsniveau.

Gezien de VS niet vallen onder de categorie van landen met een passend beschermingsniveau werd, specifiek voor de VS, bij beslissing van de Europese Commissie de Veiligehavenbeginselen ("Safe Harbour") uitgewerkt[31]. Bovendien heeft de Europese Commissie, voor wat betreft alle landen die geen passend beschermingsniveau garanderen zoals de VS , voorzien in passende contractuele bepalingen, overeenkomstig artikel 26, 2 van de richtlijn 95/46/EG[32]. Tenslotte is er het systeem van de 'Binding Corporate Rules', dit wil zeggen de interne bindende privacy gedragscode van een bedrijf, welke de transfer van persoonsgegevens naar derde landen, zonder een passend beschermingsniveau, kan voorzien. **De Commissie acht het systeem van de interne bindende privacy gedragscode ("binding corporate rules") overeenkomstig artikel 26, 2 van de richtlijn 95/46/EG een passende en vereiste maatregel om passende waarborgen te voorzien voor de dagelijkse en massale gegevenstransfers die worden verricht via de verwerkingscentra van een multinationaal bedrijf zoals SWIFT**. Zulk een gedragscode dient echter in België te zijn gemachtigd door de Koning, na advies van de Commissie.

De Commissie is van oordeel dat de bescherming die SWIFT heeft voorzien voor de verwerking van de gegevens in haar verwerkingscentrum in de VS niet voldoet aan de artikelen 21 en 22 WVP (artikelen 25 en 26 van de richtlijn 95/46/EG) **.**

E.2. <u>Pleegde SWIFT inbreuken op de WVP bij de transfer van gegevens aan de UST ?</u>

Hierna wenst de Commissie na te gaan of SWIFT de WVP geschonden heeft in het kader van de mededeling van persoonsgegevens aan de UST.

E.2.1. *Wettelijke basis (artikel 5 WVP en artikel 7 b) richtlijn 95/46/EG en artikel 8 EVRM)*

De Commissie benadrukt dat zij noch de wettelijkheid, noch de afdwingbaarheid van de Amerikaanse wetgeving en van de Amerikaanse dwangbevelen in vraag kan stellen, hetgeen duidelijk tot de bevoegdheid van de Amerikaanse overheid behoort. Wel kan zij onderzoeken of de uitvoering van de Amerikaanse dwangbevelen in het Belgische recht op de verwerking van persoonsgegevens een legitimiseringsgrond kan vinden. Op basis van artikel 5 WVP kunnen de persoonsgegevens van de opdrachtgevers of begunstigden slechts in een limitatief aantal gevallen worden verwerkt. SWIFT beroept zich niet formeel op een wettelijke basis onder Belgisch recht en verwees enkel naar de Amerikaanse dwangbevelen waarvan zij stelt de wettelijkheid en afdwingbaarheid te hebben onderzocht. Prima facie lijken echter vooral artikel 5 c) (wettelijke verplichting van de verantwoordelijke) en 5 f) (behartiging van een zwaarwegend en gerechtvaardigd belang van de verantwoordelijke) relevant om de mededeling van persoonsgegevens aan de UST te kunnen rechtvaardigen.

Wat artikel 5 c) betreft onderschrijft de Commissie de visie van de Groep 29 van 1 februari 2006 in verband met de Sarabanes-Oxley wetgeving[33]. De Groep 29 stelde reeds dat "*Een*

[31] Zie de Beschikking 2000/520/EG: van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd (Kennisgeving geschied onder nummer C(2000) 2441)

[32] Zie hieromtrent http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

[33] Zie het advies 1/2006 over de toepassing van de EU-gegevensbeschermingsregels op interne klokkenluidersregelingen in de sfeer van boekhouding, interne boekhoudcontrole, auditing en bestrijding van omkoping en van bancaire en financiële criminaliteit

verplichting uit hoofde van buitenlandse wettelijke of reglementaire bepalingen om een rapporteringssysteem tot stand te brengen, geldt daarentegen niet als een wettelijke verplichting die de verwerking van gegevens in de EU toelaatbaar maakt. Elke andere interpretatie zou het voor derde wet- en regelgevers gemakkelijk maken om de in Richtlijn 95/46/EG neergelegde EU-regels te omzeilen." Dit betekent derhalve dat de Amerikaanse dwangbevelen niet als rechtvaardigingsgrond voor gegevensverwerking conform artikel 5 c) WVP, kunnen worden beschouwd.

Aansluitend op een standpunt van de Franse Privacy Commissie (CNIL) in het SOX-dossier[34], is de Commissie wel van oordeel dat het onmogelijk is, in het geval van de Amerikaanse dwangbevelen, het gerechtvaardigd belang te negeren van SWIFT in de zin van artikel 5 f WVP. Met andere woorden, men kan niet betwisten dat SWIFT een legitiem belang heeft om zich te onderwerpen aan een geldig en uitvoerbaar dwangbevel onder Amerikaans recht. Bij niet-naleving door SWIFT van deze dwangbevelen loopt SWIFT immers het risico van burgerlijke sancties opgelegd te krijgen onder Amerikaans recht. De Commissie is derhalve van oordeel dat de transfer van gegevens aan de UST **berust op een legitiem en zwaarwegend belang in hoofde van SWIFT in de zin van artikel 5 f) WVP**.

SWIFT had zich anderzijds wel dienen te realiseren dat **de uitzonderingmaatregelen onder Amerikaans recht bezwaarlijk een geheime, systematische, massale en jarenlange inbreuk op de fundamentele Europese beginselen inzake gegevensbescherming kon rechtvaardigen bij gebrek aan afdoende duidelijke rechtvaardigingsgrond onder Europees recht**. Dit basisbeginsel kan worden teruggevonden in het tweede lid van artikel 8 EVRM[35]. De strenge basisvereisten onder dit artikel werden reeds herhaaldelijk door het EHRM toegelicht, met name bij het toetsen van geheime surveilleactiviteiten aan criteria zoals de vereiste voorzienbaarheid van de norm en de vereiste van voldoende en effectieve controlemaatregelen [36].

E.2.2. *Proportionaliteitsbeginsel (artikel 4 § 1, 3° WVP) en bewaringstermijn (artikel 4 § 1, 5° WVP)*

De Commissie is van oordeel dat in casu sprake lijkt te zijn van een "conflict of laws" situatie tussen het Amerikaans en Belgisch recht, die SWIFT dwong om moeilijke keuzes te maken na de ontvangst van de Amerikaanse dwangbevelen. In het licht van het proportionaliteitsbeginsel is het echter essentieel om na te gaan of SWIFT ook een **evenwicht heeft gezocht tussen beide rechtssystemen en hiertoe afdoende de haalbaarheid van alternatieven onder Belgisch of Europees recht heeft onderzocht en toegepast**. Het feit dat SWIFT onderworpen is aan de dwangbevelen en actief met de UST confidentiële onderhandelingen voerde over de toepassing van de dwangbevelen belet immers niet dat de verwerking dient te worden verricht in conformiteit met de beginselen onder Belgisch en Europees recht.

Gelet op het noodzakelijkheidsbeginsel is het de vraag **welke alternatieven SWIFT had eens vaststond dat zij onderwerpen was aan geldige en afdwingbare dwangbevelen**. Een aantal opties bleken voorhanden, met name :

---

[34] CNIL, Document d'orientation adopté par la Commission le 10 novembre 2005 pour la mise en oeuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.

[35] dat luidt als volgt : *"Er mag geen bemoeienis zijn van het openbaar gezag met het uitoefenen van dit recht behalve voorzover die bemoeienis overeenkomstig de wet is en noodzakelijk is in een democratische maatschappij in het belang van de nationale veiligheid, openbare veiligheid of het economisch welzijn van het land, voor het voorkomen van wanorde of misdaad, voor de bescherming van de gezondheid of de zeden, of voor de bescherming van de rechten en de vrijheid van anderen."*

[36] Zie de zaken Rotaru tegen Roemenië (§ 55 en volgende), die verwijst naar eerdere zaken zoals Malone tegen UK van 2 augustus 1984, Series A no. 82, p. 32, § 67, en *Amann* tegen Z*witserland* [GC], no. 27798/95, § 65, ECHR 2000-II, § 56):

- Het aanvechten van de dwangbevelen onder Amerikaans recht

  Op de vraag waarom de dwangbevelen niet voor de rechters in de VS werden voorgelegd antwoordde SWIFT dat de eerste dwangbevelen vlak na de gebeurtenissen van september 2001 werden ingediend. De dwangbevelen zouden actueel op een wettelijke basis onder Amerikaans recht berusten (gecodificeerd in de zgn. "Patriot Act"[37]). SWIFT stelde bovendien dat het risico bestond dat de Amerikaanse rechter zou geoordeeld hebben om SWIFT alsnog te bevelen alle data zonder beperkingen mede te delen.

- Het toepassen van de officiële procedures en verdragen inzake gerechtelijke samenwerking

  De aanbevelingen en procedures die bestaan voor gerechtelijke samenwerking op internationaal en Europees vlak en die bedoeld zijn voor de preventie van en de strijd tegen de financiering van terrorisme door toegang tot gegevens bij financiële instellingen blijken niet gevolgd.

  Hierbij kan worden verwezen naar de publieke aanbevelingen van de FATF ("GAFI")[38]. De FATF is een intergouvermenteel orgaan dat werd opgericht in 1989 en dat als doelstelling heeft om nationale en internationale beleidsmaatregelen te ontwikkelen en te promoten teneinde witwassen en de financiering van terrorisme te bestrijden. De aanbeveling nr. 40 van de FATF bevat de bepaling dat *"landen (…) controles en waarborgen (dienen) in te stellen teneinde te waarborgen dat de door de bevoegde autoriteiten uitgewisselde informatie uitsluitend op de toegestane manier wordt gebruikt in overeenstemming met hun verplichtingen inzake privacy en bescherming van persoonsgegevens."* Daarnaast kan ook worden verwezen naar de samenwerking binnen het kader van de "Egmont Groep"[39]. Via deze informele groep wordt actueel een uitwisseling van financiële informatie in werking gesteld via de operationele nationale financiële inlichtingencellen (financial intelligence units" of "FIUs") van 101 landen waaronder België en de VS. Deze uitwisseling wordt verricht via het Egmont Secure Web of "ESW").

  Voormelde alternatieve organen en systemen zouden, in het licht van de richtlijn 95/46/EG, wel aanvullende garanties kunnen bieden bij de uitwisseling van informatie inzake witwassen en de financiering van terrorisme. Tenslotte kan er op worden gewezen dat, ingevolge de aanslagen van 11 september 2001, tussen de EU en de Verenigde Staten twee internationale overeenkomsten[40] werden onderhandeld die wel werden ondertekend op 25 juni 2003 doch momenteel ter ratificatie door beide zijden voorligt. Volgens artikel 18 van het Verdrag van Wenen inzake het verdragenrecht[41] moet een Staat zich alvast onthouden van handelingen die een verdrag zijn voorwerp en zijn doel zouden ontnemen, indien hij het verdrag heeft ondertekend of de akten die het verdrag vormen heeft uitgewisseld onder voorbehoud van bekrachtiging en totdat hij zijn bedoeling geen partij te willen worden bij het verdrag kenbaar heeft gemaakt.

---

[37] De USA PATRIOT Act (Public Law 107-56) of voluit de Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 is een Amerikaans wetsvoorstel (H.R.3162) dat in 2003 door het Amerikaans Congres met een meerderheid is aangenomen. De wet heeft als doel meer mogelijkheden te geven aan de Amerikaanse overheid om informatie te vergaren over en op te treden in geval van mogelijk terrorisme. (bron : http://nl.wikipedia.org)

[38] Gepubliceerd op http://www.fatf-gafi.org. Zie http://www.fatf-gafi.org/dataoecd/42/43/33628117.PDF aangaande de 40 aanbevelingen.

[39] Zie http://www.egmontgroup.org/about_egmont.pdf

[40] "Agreement on extradition between the EU and the US" en de "Agreement on mutual legal assistance between the EU and the US". Zie de publicaties op http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf en http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20european%20union%22

[41] Verdrag van Wenen inzake het verdragenrecht, 23 mei 1969, B.S. 25 december 1993, Inwerkingtreding : 1 oktober 1992. De Verenigde Staten hebben dit verdrag ondertekend

De Commissie stelt echter vast dat **SWIFT zich beperkte tot de naleving van Amerikaans recht en het zoeken naar oplossingen via geheime onderhandelingen met de UST.** De Commissie betreurt hierbij dat nooit werd gekozen om de toepassing van voormelde alternatieven te onderhandelen en de bevoegde Europese autoriteiten[42] inzake gegevensbescherming te contacteren teneinde de massale transfer van persoonsgegevens aan de UST ook onder Europees recht te toetsen.

Wat de toepassing van het proportionaliteitsbeginsel betreft merkt de Commissie op dat de massale, geheime, jarenlange en systematische doorgifte van persoonsgegevens ook kan worden beschouwd als een inbreuk op artikel 4 §1, 3° WVP.

Tenslotte dient ook de controle op de bewaringstermijn van de gegevens in de zwarte doos essentieel te worden geacht in het licht van de naleving van het proportionaliteitsbeginsel. Wat de bewaringstermijn betreft van de gegevens wordt een onderscheid gemaakt tussen de normale bewaringstermijn die gebruikelijk is in het kader van de normale werking van de SWIFT verwerkingscentra en de bewaringstermijnen die gelden voor de data in de zwarte doos die ter beschikking wordt gesteld aan de UST[43]. Uit verificatie van de afspraken tussen SWIFT en de UST blijkt dat er sprake lijkt te zijn van een **bewaringstermijn voor onbepaalde duur**, dus ruim na de normale bewaringstermijn in het kader van de dienst SWIFTNet FIN, hetgeen strijdig is met het proportionaliteitsbeginsel. Aanvankelijk bestond de mogelijkheid om berichten te bewaren in de zwarte doos zolang als zij een mogelijk nut vertoonden voor een onderzoek. Nadien werd de mogelijkheid voorzien voor SWIFT om van de UST alle niet-opgehaalde berichten uit de zwarte doos terug te halen, zij het onder de verplichting om deze data te bewaren voor zolang als de mogelijkheid bestaat dat een dwangbevel zou worden uitgevaardigd over deze data (zie supra onder B.4.1.)). De Commissie stelt vast dat deze “verplaatsingsmogelijkheid” van data (van de zwarte doos naar SWIFT) weinig invloed uitoefent op de eigenlijke bewaringstermijn, die in principe onbepaald blijft, met name zolang als de mogelijkheid van een dwangbevel op deze data bestaat. De Commissie merkt tenslotte op dat vooralsnog geen concrete onafhankelijke verificaties konden worden uitgevoerd in verband met de concrete bewaringstermijn van data in individuele gevallen. Het kan derhalve niet worden uitgesloten dat persoonsgegevens jarenlang zonder onafhankelijke verificatie kunnen worden bewaard in de zwarte doos.

Op basis van voormelde overwegingen is de Commissie van oordeel dat voormelde praktijk van massale, geheime, jarenlange en systematische doorgifte van persoonsgegevens aan de UST met een onbepaalde bewaringstermijn **een inbreuk vormt op de beginselen van proportionaliteit en beperkte bewaringstermijn zoals verwoord in de artikelen 4 §1, 3° WVP (proportionaliteit) en 4 § 1, 5° (bewaringstermijn) WVP ingevolge de artikelen 6.1. (c) en 6.1. (e) van de richtlijn 95/46/EG. Als verantwoordelijke had SWIFT zich hierbij dienen te realiseren dat deze beginselen fundamenteel worden geacht in de Europese rechtsorde.**

E.2.3. *Finaliteitsbeginsel*

De Commissie benadrukt dat zij het belang en de legitimiteit erkent van de wereldwijde strijd tegen het terrorisme. Cruciaal bij de evaluatie in het licht van de WVP is echter of de dwangbevelen, gelet op hun bewoordingen, inderdaad slechts voor terrorismebestrijding konden worden gebruikt, en bijvoorbeeld geen machtiging inhielden voor andere doeleinden, zoals werd gesuggereerd in bepaalde media[44]. Dit aspect hangt af van de

[42] Rekening houdend met de analyse van de overseeërs die zich reeds in 2002 onbevoegd verklaarden in de materie van de dwangbevelen.

[43] De bewaringstermijnen die UST zou hanteren over de data die zij na extractie uit de zwarte doos heeft vergaard zijn onbekend.

[44] Zie bijvoorbeeld een artikel in Knack van 9 augustus 2006 waarin de auteur suggereert dat er sprake zou zijn van zaken die geen verband zouden met terrorisme zoals “een drugsgerelateerde zaak”.

definitie en communicatie van de doelstelling van de verwerking via de informatieplicht, die hierna wordt toegelicht.

Het behoort echter niet tot de bevoegdheid van de Commissie om de legitimiteit en het gerechtvaardigd karakter van de Amerikaanse dwangbevelen in vraag te stellen.

E.2.4. *Informatieplicht in hoofde van SWIFT (artikelen 4 § 1, 2° en 9 § 2 WVP en artikel 8 EVRM)*

De Commissie stelt vast dat elke controle op de finaliteit staat of valt met de vereiste transparantie en de precieze definitie van de doelstellingen van de verwerking. Zij merkt dienaangaande op dat:

- de exacte doelstelling van de verwerking (bestrijden van terrorisme) in beginsel werd opgelegd en gedefinieerd in de dwangbevelen waarvan de exacte doelstelling steeds met de grootste confidentialiteit en non-transparantie werd behandeld;
- de doelstellingen die werden verwoord in de communicaties van SWIFT naar het algemene publiek voor 23 juni 2006 (en dus naar de betrokkenen toe) zeer vaag bleven en geen duidelijk verband werd vermeld met terrorisme (vermelding van "illegale activiteiten" en "illegaal gedrag" in het publieke compliance beleid van SWIFT)
- dat pas in de algemene perscommuniqués van na 23 juni 2006 herhaaldelijk werd gepreciseerd dat SWIFT de data enkel meedeelde voor "specifieke terrorismeonderzoeken" (in de verklaring in verband met co mpliance van 23 juni 2006 en de updates na deze datum van deze verklaring)

De Commissie stelt verder vast dat het "geen commentaar" beleid van SWIFT inzake compliance op gespannen voet blijkt te staan met de transparantievereiste die volgt uit de richtlijn 95/46/EG en het tweede lid van artikel 8 EVRM. Dit beleid lijkt grotendeels ingegeven te zijn door de strenge confidentialiteitsverplichtingen die werden opgelegd aan SWIFT in het kader van individuele onderzoeken van de UST, de algemene regels van confidentialiteit en discretieplicht die gelden in de wereld van de financiële dienstverlening en tenslotte de commerciële belangen en het reputatierisico van SWIFT.

De kiese vraag moet echter worden gesteld **waar het evenwicht dient te worden gevonden tussen de hoge graad van confidentialiteit** die door SWIFT werd **verleend aan het systeem en de omvang van de verwerkingen ingevolge de dwangbevelen en anderzijds de diverse transparantieverplichtingen die SWIFT als verantwoordelijke** draagt onder de artikelen 4 § 1, 2° WVP (vereiste definitie van de finaliteit in het privacybeleid) en 9 § 2 WVP (informatieplicht) . Anderzijds is het de vraag tot op welke hoogte SWIFT de financiële instellingen en de betrokkenen kon én diende te informeren ingevolge artikel 9 § 2 WVP over de transfer aan de gegevens via de UST.

De Commissie is er zich van bewust dat wettelijke of conventionele confidentialiteitsverplichtingen bestaan, zowel voor de situatie van de Amerikaanse dwangbevelen als voor de Belgische dwangbevelen, waardoor de normale informatieplicht ten aanzien van de betrokken natuurlijke persoon (verdachte, die het voorwerp uitmaakt van het dwangbevel), niet altijd van toepassing zal zijn bij de uitvoering van een dwangbevel.

De Commissie wijst echter op een fundamenteel verschil dat de dwangbevelen van de UST onderscheidt van de dwangbevelen onder Belgisch recht. Onder rubriek B.2. werd reeds opgemerkt dat de dwangbevelen van de UST moeten gekwalificeerd worden als **niet geïndividualiseerde massale opvragingen ("Rasterfandung" "carpetsweeping" techniek)** die in twee trappen werken, hetgeen verschillend is van de Belgische dwangbevelen die *ab initio* per individueel geval worden uitgeoefend. Er werd onder rubriek B.2. in fine ook opgemerkt dat de UST "het volle recht heeft onder Amerikaans recht om **alle** SWIFT boodschappen mede te delen. Dit betekent dus dat, alleen voor het jaar 2005, een totaal van 2.518.290.000 SWIFTNet Fin boodschappen per jaar aan de dwangbevelen

kan worden onderworpen[45] SWIFT stelt echter het exacte aantal gegevens in de zwarte doos enkel te kunnen vrijgeven na het toepassen van een machtigingsprocedure met de UST.

Gelet op het tweede lid van artikel 8 EVRM **blijven de transparantieverplichtingen wel op het collectieve niveau bestaan**, dus wat betreft het fenomeen van de massale opvragingen via Europese of Amerikaanse dwangbevelen.

Rekening houdende met het geheim, massaal en ongewoon karakter van de gegevenstransfer is de Commissie derhalve van oordeel dat SWIFT minstens de financiële instellingen en de toezichthoudende overheden inzake gegevensbescherming (Europese autoriteiten, DPA's waaronder de Commissie) op de hoogte diende te stellen van de dwangbevelen van de UST.

E.2.5. *Aangifteplicht*

Krachtens artikel 17 § 6 WVP moet een doorgifte van persoonsgegevens aan het buitenland aangegeven worden. SWIFT verrichte deze aangifte wel voor tal van andere verwerkingen[46] doch niet voor de transfer van gegevens naar de VS en evenmin voor de finaliteit "compliance". Dit is merkwaardig nu het zeker niet ongebruikelijk is voor financiële instellingen en andere financiële dienstverleners zoals SWIFT om hun "compliance-finaliteit" en internationale transfers afzonderlijk aan te geven bij de Commissie. Zo zijn verwijzingen naar "compliance" verwerkingen ingevolge de Wet van 11 januari 1993[47] vrij courant in hoofde van verantwoordelijke financiële instellingen.

Door de gegevenstransfers aan de VS en de compliance finaliteit in het kader van de dwangbevelen niet te vermelden in de aangifte **pleegde SWIFT een inbreuk op de artikel 17 § 1 WVP.**

E.2.6. *Vereiste van onafhankelijke controle op de gegevenstransfer (artikel 28 richtlijn 95/46/EG en artikel 8 EVRM)*

Enkel het bestuur van SWIFT bleek voor de persberichten van juni 2006 in België op de hoogte van de modaliteiten van de doorgifte aan de UST[48]. De onafhankelijke controle die vereist wordt ingevolge artikel 28 Richtlijn 95/46/EG blijkt dus grotendeels belemmerd door het feit dat de massale gegevenstransfers door SWIFT met de grootste mate van confidentialiteit werden behandeld. Aldus werden noch de betrokken financiële instellingen, noch de bevoegde Europese overheden inzake dataprotectie op de hoogte gesteld van het massale fenomeen van de Amerikaanse dwangbevelen.

De vereiste van onafhankelijke controle volgt echter ook uit het tweede lid van artikel 8 EVRM. In de zaak Rotaru stelde het EHRM : "De rechtsnorm impliceert, onder meer, dat een inbreuk door administratieve overheden met de rechten van een individu het voorwerp dienen uit te maken van een effectieve supervisie, die normaal gesproken dient te worden uitgeoefend door de rechterlijke macht, tenminste in laatste instantie, sinds de rechterlijke

[45] Cijfer vermeld in hetzelfde schrijven van SWIFT van 14 september 2006. Men kan ook uitgaan van een gemiddeld en normaal dagelijks berichtenverkeer via SWIFTNet FIN dat tussen 6,9 miljoen (2005) en 11 miljoen berichten per dag (begin 2006) bedraagt en dat in zijn totaliteit aan de dwangbevelen kan onderworpen worden.

[46] Met name ledenbeheer, klantenbeheer,…

[47] Wet tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van het terrorisme

[48] los van het feit dat de NBB als "lead overseer" op de hoogte werd gebracht van het bestaan van het eerste dwangbevel en dat de financiële instellingen welbekend mogen worden geacht met de praktijk van dwangbevelen en het feit dat de SWIFT transacties volgens de contractuele documenten aan deze bevelen onderworpen werden geacht.

controle de beste garanties biedt van onafhankelijkheid, onpartijdigheid en een behoorlijke procedure (...)"[49]

Bij de instandhouding van de massale en geheime surveille zonder medeweten van de bevoegde Europese overheden inzake gegevensbescherming, en zonder onafhankelijke controle binnen de VS (de enige controle werd door ondernemingen in de privé sector doorgevoerd, zijnde SWIFT en haar auditor) **werd een inbreuk gepleegd op de vereisten onder artikel 28 van de richtlijn 95/46/EG.**

E.2.7. *Doorgifteverbod bij verdere transfers aan ontvangers van gegevens zoals de UST (artikelen 21 WVP en 25 en 26 van de richtlijn 95/46/EG)*

Bij gebrek aan toepasselijke uitzonderingsbepalingen in de zin van artikelen 22 WVP en 26 van de richtlijn 95/46/EG (zie supra), wijst de Commissie op het feit dat de transfer van gegevens aan de UST geenszins afdoende kan worden geregulariseerd via het afsluiten van "contractuele bepalingen" of "binding corporate rules" binnen de SWIFT groep.

Net zoals in het PNR-precedent[50] lijken voor deze zogenaamde verdere doorgiftes ("onward transfers") specifieke overeenkomsten tussen de VS en de EU vereist teneinde er alsnog voor te zorgen dat de ontvanger van de gegevens (UST) de regels van de passende bescherming onder Europees recht afdoende zal aanvaarden. Dit is de strekking die de Groep 29 verleent aan de artikelen 25 en 26 van de richtlijn 95/46/EG[51]. Voor SWIFT hadden de bestaande GAFI akkoorden als uitgangspunt kunnen worden gebruikt, doch het is de vraag waarom deze optie niet werd genomen.

Gelet op het feit dat de ontvanger van de gegevens (UST) nooit werd onderworpen aan passend beschermingsniveau conform artikel 21 WVP en de richtlijn 95/46/EG, is de Commissie van oordeel dat SWIFT **artikel 21 § 1 WVP heeft geschonden**. Het kan hierbij als een grove inschattingsfout worden beschouwd in hoofde van SWIFT om jarenlang op geheime en systematische wijze een massale hoeveelheid persoonsgegevens aan de surveille door de UST te onderwerpen zonder tegelijk de bevoegde Europese overheden en de Commissie te hebben gecontacteerd teneinde een oplossing onder Belgisch en Europees recht te bekomen.

OM DEZE REDENEN,

Op basis van haar algemeen onderzoek is de Commissie van oordeel dat:

- de WVP van toepassing is op de gegevensuitwisseling via de dienst SWIFTNet FIN;

- SWIFT en de financiële instellingen gezamenlijke verantwoordelijkheid dragen in het licht van de WVP voor de verwerkingen van persoonsgegevens via de dienst SWIFTNet FIN;
- SWIFT een verantwoordelijke is voor de verwerking van persoonsgegevens die via de dienst SWIFTNet FIN worden verwerkt;

---

[49] "*The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55)."*

[50] Sinds begin januari 2003 eisten de Verenigde Staten toegang tot de Passenger Name Records (de reis- en boekingsgegevens of "PNR") van alle passagiers op vluchten van, naar of via de VS.. Sindsdien worden op Europees vlak oplossingen gezocht voor de vereiste van het passend beschermingsniveau bij de doorgifte van deze gegevens aan de Verenigde Staten van Amerika.

[51] Zie het werkdocument van 24 juli 1998 van de groep 29 betreffende de doorgifte van persoonsgegevens naar derde landen : toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming, gepubliceerd op http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1998_en.htm

- de financiële instellingen verantwoordelijk zijn gezien zij in het interbancaire verkeer mede het doel en de middelen bepalen van de uitvoering van de betalingsopdrachten. Dat de financiële instellingen met name op interbancair vlak financiële berichten in verband met deze betalingsberichten via de dienst SWIFTNet Fin laten verwerken;

- wat de normale verwerking van persoonsgegevens in het kader van de dienst SWIFTNet Fin betreft, had SWIFT haar verplichtingen onder de WVP dienen na te leven, waaronder de informatieplicht, de aangifteplicht en de verplichting om te voorzien in een passend beschermingsniveau conform artikel 21 § 2 WVP;

- wat de mededeling van persoonsgegevens aan de UST betreft, is de Commissie van oordeel dat SWIFT zich in een conflictsituatie tussen Amerikaans en Europees recht bevindt en minstens een aantal inschattingsfouten beging bij de behandeling van de Amerikaanse dwangbevelen. Dat het met name als een grove inschattingsfout moet worden beschouwd in hoofde van SWIFT om jarenlang op geheime en systematische wijze een massale hoeveelheid persoonsgegevens aan surveille te onderwerpen zonder een afdoende en duidelijke rechtvaardigingsgrond en onafhankelijke controle in overeenstemming met Belgisch en Europees recht. In deze context had SWIFT van bij het begin bewust dienen te zijn van het feit dat, naast de toepassing van het Amerikaans recht, ook de fundamentele beginselen onder Europees recht dienen te worden nageleefd, zoals het proportionaliteitsbeginsel, de beperkte bewaringstermijn, het transparantiebeginsel, de vereiste van onafhankelijke controle en de vereiste van een passend beschermingsniveau. Deze vereisten worden immers verwoord in het tweede lid van artikel 8 EVRM, het Verdrag nr. 108, de richtlijn 95/46/EG en de WVP en zijn op SWIFT van toepassing. De Commissie verwijst ook naar het internationaal precedent in het PNR-dossier. De overheden die bevoegd zijn inzake gegevensbescherming (de Commissie, haar ambtsgenoten en de Europese Commissie) hadden van bij het begin geïnformeerd dienen te worden, waardoor het mogelijk had kunnen zijn om op Europees vlak een oplossing uit te werken voor de mededeling van persoonsgegevens aan de UST, met respect voor voormelde beginselen die gelden onder Europees recht. Hiertoe had eveneens de Belgische regering kunnen worden aangeschreven teneinde om een initiatief op Europees vlak te verzoeken.

Gelet op de complexe materie en het belang ervan, houdt de Commissie zich verder ter beschikking voor het verlenen van verder advies in deze aangelegenheid.

De administrateur, Gelet op de verhindering van de voorzitter,
De vice-voorzitter,

(get.) Jo BARET (get.) Willem DEBEUCKELAERE