Medlemmerne af Folketingets Europaudvalg
og deres stedfortrædere

Asiatisk Plads 2
DK-1448 København K
Telefon +45 33 92 00 00
Telefax +45 32 54 05 33
E-mail: um@um.dk
http://www.um.dk
Girokonto 3 00 18 06

| Bilag | Journalnummer | Kontor | |
|---|---|---|---|
| 1 | 400.C.2-0 | EUK | 24. august 2010 |

**SVAR PÅ UDVALGSSPØRGSMÅL**

**SWIFT-data**

Til underretning for Folketingets Europaudvalg vedlægges Økonomi- og Erhvervsministeriets besvarelse af spørgsmål nr. 11-12 ad KOM (2009) af 13. juli 2010 vedrørende SWIFT-data.

Lene Espersen

ØKONOMI- OG ERHVERVSMINISTERIET

ØKONOMI- OG
ERHVERVSMINISTEREN

23. august 2010

ØKONOMI- OG
ERHVERVSMINISTERIET
Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax 33 12 37 78
CVR-nr 10 09 24 85
oem@oem.dk
www.oem.dk

**Besvarelse af spørgsmål 12 ad KOM (2009) 0703 stillet af Europaudvalget den 13. juli 2010 efter ønske fra Per Clausen (EL).**

**Spørgsmål:**
Den afvejning, ministeren må have foretaget, har under alle omstændigheder handlet om proportionaliteten mellem terrorbekæmpelseshensynet på den ene side og privatlivsbeskyttelseshensynet på det andet. Datatilsynet har tidligere kritiseret masseudleveringen som værende i strid med dette proportionalitetsbegreb. Det er siden blevet påvist, at "bulk udlevering" anvendt til at finde terrorister ud fra en samkøring af forskellige data såsom internetadfærd, email overvågning, flyrejsemønstre og betalinger, ikke har nogen praktisk værdi. Mener ministeren, at han har været berettiget til uden præcist at orientere folketinget at komme til det resultat, at bulkudlevering uden videre kan finde sted uanset EU's position?

**Svar:**
Netop begrænsning af udlevering af bulk-oplysninger har været et væsentligt punkt for Europa-Parlamentet, der med godkendelsen af aftalen har fundet, at problemet er løst tilfredsstillende. Jeg henviser desuden til svaret på spørgsmål 5, hvoraf det fremgår, at udgangspunktet er, at det i videst muligt omfang skal undgås, at der anmodes om data med karakter af bulk-data. Hvis mistanken om terrorisme er stærk nok, og US Treasury klart (clearly substantiate the necessity) kan begrunde behovet for de pågældende data, jf. aftalens ordlyd, kan der dog udleveres data, der ikke er relateret til en enkelt transaktion under aftalen.

Med hensyn til spørgsmålet om, hvorvidt udlevering af bulk-data kan være af praktisk værdi, har jeg forelagt spørgsmålet for Finanstilsynet, der har erfaringer med overvågning af transaktioner. Finanstilsynet anfører, at udlevering af bulk-data i visse tilfælde har en praktisk værdi. Ofte forsøges ulovlige transaktioner skjult på forskellig måde, og en gennemgang af større dataserier kan f.eks. afsløre mønstre i betalinger, der kan føre til afsløring af ulovlige transaktioner. Det kan f.eks. være en række små beløb, der fordeles over flere forskellige pengeinstitutter og til flere forskellige modtagere. Da Danmark ikke er en del af aftalen, har vi fra dansk side dog ikke foretaget en konkret vurdering af behovet for at sende bulk-data. Da der ikke er foretaget en konkret dansk vurdering, har Folketinget heller ikke modtaget en sådan vurdering.

Det fremgår imidlertid af aftalen, at af hensyn til datasikkerheden kan ingen oplysninger udleveres under aftalen, uden at det er specificeret, hvilke oplysninger der anmodes om, ligesom det skal være underbygget, at oplysningerne er nødvendige i en konkret efterforskning. Desuden skal

alle udleveringer godkendes af Europol. Endelig er alle betalinger via SEPA undtaget. Der er således ikke tale om, at bulk-udleveringer "uden videre" kan finde sted. Fra dansk side har vi været positive overfor de begrænsninger, der på den måde ligger i udleveringen af data, herunder bulk-data.

Jeg har forstået på Datatilsynet, at Datatilsynet deltager i den arbejdsgruppe, der er nedsat i henhold til art. 29 i databeskyttelsesdirektivet (direktiv 95/46/EF) den såkaldte "Artikel 29-gruppe".

Gruppen er rådgivende og uafhængig, og den består af repræsentanter fra den eller de tilsynsmyndigheder, som hver medlemsstat har udpeget, af en repræsentant fra den eller de myndigheder, der er oprettet for fællesskabsinstitutionerne og -organerne, samt af en repræsentant for Kommissionen.

Jeg er blevet bekendt med, at Artikel 29-gruppen den 25. juni 2010 – dvs. inden vedtagelsen af aftalen - sendte et brev til Europa Parlamentet, hvor Artikel 29-gruppen anmoder Europa-Parlamentet om at adressere spørgsmålet om databeskyttelse inden vedtagelsen af aftalen. Spørgsmålet om bulk udleveringer af data blev også berørt. Europa-Parlamentet har som bekendt efterfølgende godkendt aftalen.

En kopi af brevet til Europa-Parlamentet vedlægges.

ARTICLE 29 Data Protection Working Party

Working Party on Police and Justice

Brussels, 25/06/10
JLS-D5 D(2010) 10038

Mr. Juan Fernando LÓPEZ AGUILAR
Chairman of the Committee on Civil Liberties, Justice and Home Affairs
European Parliament
B-1047 Brussels

Dear Mr. López Aguilar,

We refer to our letter of 22 January 2010 in which the Article 29 Working Party and the Working Party on Police and Justice examined the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States of America for the purposes of the Terrorism Finance Tracking Program ("TFTP 1 agreement"). Both Working Parties are pleased with the fact that data protection concerns played a big part in the no-vote against the TFTP1 agreement on 11 February 2010.

On 28 May 2010, the subgroup on financial matters of the Article 29 Working Party was briefed by the services of the European Commission, DG Justice, Liberty and Security. The members of the subgroup assessed the draft negotiating directives adopted in March 2010 to negotiate a new TFTP agreement (hereafter "draft negotiating directives TFTP2), and the document titled "Agreement between the European Union and the United States of America on the processing and Transfer of Financial Messaging Data From The European Union To The United States for Purposes of the Terrorist Finance Tracking program", hereafter "TFTP2 Agreement". Both documents were published[1].

[1] Published under official references COM (2010) 316 and 317 of 11 June.

Despite the additional attention that is clearly given to data protection, we are as yet unsure about the outcome. Still, the European Data Protection Authorities (DPAs) feel compelled to convey to you again what we see as important data protection issues that appear from our first reading of the TFTP2 Agreement.

We hereby enclose our initial assessment carried out by the Article 29 Working Party and the Working Party on Police and Justice. We trust that our point of view will continue to receive due consideration by the European Parliament in its future deliberations on the TFTP2 agreement. Of course, we remain at your disposal for further information on this issue if so required by the Parliament

Furthermore, both Working Parties plan to fully assess the TFTP2 agreement once signed by the negotiating partners and made public by the European Commission. Should this lead to further concerns, we will of course make those clear, either by letter or in a formal opinion.

Yours sincerely,

| | |
|---|---|
| Jacob Kohnstamm | Francesco Pizzetti |
| Chairman of the Art. 29 Working Party | Chairman of the Working Party on Police and Justice |

Enclosure: Assessment of the Article 29 Working Party and the Working Party on Police and Justice

Cc: Mr. Jerzy Buzek, President of the European Parliament
Ms Viviane Reding, Vice-President of the European Commissioner responsible for Justice, Fundamental Rights and Citizenship
Ms Cecilia Malmström, Commissioner for Home Affairs
Mr. Jonathan Faull, Director General (DG Justice, Freedom and Security) European Commission
Mr. Pérez Rubalcaba (Minister of Interior, ES)
Mr. Caamaño Domínguez (Minister of Justice, ES)

## Attachment

### Background

The Terrorist Finance Tracking ("TFTP") Program is a US government program that allows different US authorities to access the SWIFT transaction database. The existence of this program was revealed by the media in June 2006, and was followed by an Opinion of the WP29[2] of 22 November 2006.

Since the beginning of 2010, SWIFT has implemented their "distributed architecture" whereby intra-European messages are only processed and stored in their EU operational centres (in The Netherlands and Switzerland), and no longer in the US.

On 11 February 2010, the European parliament issued a negative vote on the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States of America for the purposes of the Terrorism Finance Tracking Program ("TFTP 1 agreement").

On 5 May 2010 the European Parliament adopted a Resolution on the recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the European Union and the United States of America to make available to UST financial messaging data to prevent and combat terrorism and terrorist financing (TFTP2 Agreement). The TFTP2 Agreement reaffirms new elements such as the possibility of an EU TFTP program[3] and the possibility of extension from SWIFT to other providers of financial data[4].

Finally, despite the new distributed architecture of SWIFT, different EU authorities received early 2010 the confirmation that at least one UST subpoena was issued over both US and EU data, including messaging data related to SEPA transactions.

### First Assessment of the Article 29 Working Party and the Working Party on Police and Justice of the TFTP2 Agreement).

The Article 29 Data Protection Working Party (WP29) carried out an assessment of the public versions of the draft negotiating directives TFTP2 and the TFTP2 Agreement, published under references COM (2010) 316 and 317 of 11 June.

In addition, the Working Party on Police and Justice (WPPJ) discussed the TFTP2 Agreement at its meeting of 23 June 2010 and expressed concurrence with this first assessment of the WP29.

This document contains the initial response of WP29 and WPPJ to the TFTP2 Agreement.

---

2 See Opinion WP 128 nr. 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), published on http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm

3 Article 11 of the TFTP2 Agreement

4 Article 11 contains the wording "the Parties shall actively pursue, on the basis of reciprocity and appropriate safeguards, the cooperation of any relevant international financial payment messaging service providers"

**Additional guarantees**

The WP29 and WPPJ welcome the fact that the TFTP2 Agreement contains additional safeguards regarding data protection. These safeguards enhance amongst others the data quality[5]. The agreement provides for "administrative redress on a non-discriminatory basis and the availability of a process for seeking judicial redress under U.S. law, regardless of nationality or place of residence"[6], and a data retention scheme. Also, Article 13.3 states that The European Union joint review delegation shall include representatives of two data protection authorities, at least one of which shall be from a Member State where a Designated Provider is based.

**Additional concerns**

However, in addition to the points raised in their joint letter of 22 January 2010, the WP29 and WPPJ would like to express a number of points that, as they understand, are not (yet) sufficiently dealt with in the TFTP2 Agreement. Despite recent assessments in official press releases from EU side that refer to "significant data protection provisions"[7] under the TFTP2 Agreement, the WP29 and WPPJ are of the opinion that these open points still imply serious data protection risks.

1. **Scope of the agreement: unclear status of protection of SEPA data in EU operational centers, retroactive application to data subject to subpoenas before the entry into force of TFTP2**

Since WP29 and WPPJ received confirmation that (SEPA and other) data in EU operational centers fall under the competence and scope of UST subpoenas[8], we question why article 4.2 (d) of the TFTP2 Agreement contains the explicit statement that ""The Request (together with any supplemental documents) shall: (…) (d) not seek any data relating to the Single Euro Payments Area". The WP29 and WPPJ assume this statement is either a misrepresentation or a confirmation of the intention to exclude the SEPA data in EU operational centers from the scope of US Subpoenas.

In order to have an agreement that provides real and effective data protection, the WP29 and WPPJ find that it is the most privacy compliant option to exclude SEPA data from US Subpoenas via a clear US commitment to exclude SEPA data. However, the WP29 and WPPJ are also aware that today such data fall under the power of the UST to issue subpoenas, and therefore, as a minimum data protection and privacy compliance requirement, the purpose of the TFTP2 Agreement should be at least to protect all data that is contained in the EU operational centers of all financial payment messages providers that could (in the future) fall under the TFTP2 Agreement.

The WP29 is of the opinion that the status of the data received and still stored under subpoena's that were issued before the entry into force of the TFTP2 Agreement should be addressed. Retroactive application of the TFTP2 Agreement to cover subpoenas served before the date of

---

5 See Article 5.6. and 5.7 that refers to motivation (nexus) and logging for each individual search, and the assessment of the subpoena's by the UST and by a public authority

6 See page 4 of the Agreement (explanatory memorandum) , and articles 4.8, 14, 15.3 and 16.2

7 See the press release of 10 June of the EU Commissioner for Home Affairs that refers to "considerable improvements", "significantly stronger data protection guarantees", and "a substantial improvement as compared to the rejected interim agreement"

8 Different EU authorities have received a letter of the concerned provider for financial payment messages where it was stated that a UST subpoena was received that covers also data in their EU operational center.

entry into force of TFTP2 should be excluded, as the TFTP2 agreement only provides a legal basis for data obtained under subpoenas that were issued after a valid EU legal basis and adequate data protection guarantees were put in place. Such was clearly not the case for older data received under the previous EU-US arrangements (representations and TFTP1 Agreement). However, data that were obtained under the TFTP1 Agreement are still taken aboard under the TFTP2 Agreement, and made subject to a retroactive application of the five year data retention mechanism. This may – de facto – go beyond the 5 year time limit (see article 6.3).

## 2. Necessity and proportionality : the transfer of bulk data continues and legal alternatives

As put forward in our letter of 22 January, we stress the fact that, for technical reasons, the designated provider is not able to identify and produce specific data in reply to UST subpoenas.

Even though the categories of data would now be specified under the TFTP2 Agreement[9], the data is still transferred in bulk to the US.

In our view, technical difficulties are not a sufficient justification of bulk transfers of data of EU- and non-EU-citizens.

The TFTP2 Agreement fails to justify why the combined application of existing cooperation mechanisms between EU and US for the intended purposes are inadequate, such as via the Egmont Group and the mutual legal assistance between the European Union and the United States of America of 25 June 2003[10], that entered into force on 1 February 2010.

Also, even if data would be grouped in categories like in the PNR file, bulk transfers create additional problems such as increased problems of correct extraction of data, the increase of the backlogs to properly control and assess the accuracy of all data that is transferred and extracted (often controls are limited to samples or ad hoc controls due to understaffing of the control or audit departments), and a lack of timely compliance with access or rectification requests. Such problems in processing operations for antiterrorism purposes were already publicly reported by US authorities such as DHS[11] and the US Department of Justice[12]. Therefore, bulk transfers can easily undermine the effective realisation of the purposes under the TFTP2 Agreement.

---

[9] General reference to categories of data in article 4.2. (a) regarding the request. Nonetheless, it also has to be noted that, according to the negotiating directives for TFTP2 Agreement, an **exhaustive list of categories of data affected by the request** should have been previously **indicated in the Annex of the TFTP2 Agreement** (point 2, second sentence, of the negotiating directives, stating that "The Annex should contain an exhaustive list of categories of data affected by the request"). Contrary to the mandate, Article 3 of the TFTP2 lays down that "The Designated Providers shall be identified in the Annex to this Agreement", without mentioning (categories of) Provided Data.
Considered the purpose of the Agreement (including investigation and prosecution for alleged terrorism and/or terrorism financing), it is of paramount importance to provide **exact, clear and strict definitions** of the scope of **"**financial payment messaging and related data". The concern is even more alarming if we take into account that, pursuant to art. 5.7, such data may include sensitive data, and that the TFTP2 does not provide specific safeguards for such data, apart a declaration that "the US Treasury Department shall protect such data in accordance with the safeguards and security measures set forth in this Agreement and with full respect and taking due account of their special sensitivity."

[10] Official Journal, 19 July 2003, L 181/34

[11] The Privacy Office of the U.S. Department of Homeland Security (DHS) released in the second part of December 2008 a report regarding the Passenger Name Record (PNR) information from the EU-US flights. This report referred to a backlog and stated that the requests for PNR took more than one year to process and were inconsistent in what information was redacted. See page 26 of the report published on http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf )

[12] See the US Department of justice, Office of the Inspector General, Audit Division, Audit Report 07-41 of September 2007 (follow-up audit of the Terrorist Screening Center, hereafter "TSC") that relates to the TSC's consolidated terrorist screening database (TSDB). The summary of the report (page 3) indicated inaccurate watchlist records and continued

The WP29 and the WPPJ conclude that it still remains to be assessed whether the bulk transfer of data via specified categories under a new legal instrument can comply with the necessity and proportionality requirements.

### 3. Gaps in the existing independent oversight and control mechanisms by EU data protection authorities and EU judicial authorities

According to article 28 of the Directive 95/46/EC, authorities should be completely independent with full powers vis-à-vis all aspects of data protection operations. This standard was recently upheld by the European Court of Justice[13].

The TFTP2 Agreement should not limit the supervisory competence and powers of data protection authorities, which are competent for the supervision of data processing. However instead, TFTP2 Agreement contains several limitations to the above standard and principle.

First, the independent, full power of oversight and control of DPAs and judicial authorities is not fully implemented under the TFTP2 agreement. Some of the existing oversight competences under article 28 of the Directive 95/46/EC are instead separated and transferred to other levels.

These competences concern different powers of DPA's (1) to obtain all relevant information, (2) to independently assess such information of (3) full data protection compliance and, subsequently, (4) the possibility to either give binding legal effect to data transfers from national processing operations under a UST subpoena on EU territory, or where necessary, to order the blocking of such transfers :

(1) **the possibility to give binding legal effect to such order related to national data processing operations**, or, where deemed necessary, to block such data transfer based on national data processing operation is replaced by an European verification and assessment mechanism (article 4.4. of the Agreement).

(2) the power to make **a full data protection assessment** in the light of all requirements of the Directive 95/46/EC is not foreseen. Instead, article 4.4. of the Agreement provides for a limited data protection assessment by Europol of the production order ("request") in the light of a limited number of criteria mentioned in article 4.2

(3) the power to make an independent assessment is not implemented. Europol is not required to be **completely independent**, and may even lack concern in the matter of data protection.

(4) In the absence of a fully independent US DPA[14], the exercise of the **full investigative power to request all information** (amongst others related to handling access and rectification requests or to exercising the other tasks) is not granted to DPAs. Instead, article 15.3 of the Agreement states that the "Privacy Officer of the U.S. Treasury Department",(…) "shall make all necessary verifications pursuant to the request". The EU DPA's are to simply pass on the request of the data subject to the UST. Hence, an important level of assessment of access requests remains with the UST and

---

weaknesses in data management due to different interconnected databases and significant increase in (also duplicate) records that have to be verified. Ie. There is a proven link between risk for inaccuracy of data and

13 Case C-518/07, *Commission of the European Communities v Germany*, delivered on 22 October 2009

14 It might be sufficient if such power was granted to a fully independent DPA in the US, which would then collaborate with EU DPAs. Since this is not the case, strong safeguards on US side and extensive competence of EU DPAs appear necessary.

misrepresentations cannot be controlled by DPAs. It is unclear why indirect access rights cannot be granted, as is the current standard in several EU members for the verification by DPAs of police and intelligence processing operations, including processing operations for antiterrorism and anti money laundering purposes. In any case, EU DPAs are under this procedure unable to independently establish whether or not the conditions of the TFTP2 Agreement are fulfilled and give full guarantees to the individual making the request.

The quality of oversight "in real time" is determined by UST[15] and there is no independent oversight by judicial EU authorities in accordance with European data protection standards[16]. Data handling would continue to be mainly verified "in real time" by the existing "SWIFT" scrutinizers, that would now only be controlled from time to time by the European Commission[17].

The WP29 and WPPJ are of the opinion that only an independent EU public authority could meet the current EU oversight standard and therefore can fulfil the different roles of oversight and control as foreseen in the TFTP2 Agreement. Currently, control by an independent judicial EU authority appears to be an essential requirement to offer adequate guarantees for the respect of data protection principles set out in the Directive 95/46/EC.

The choice for EU police authorities such as Europol is deemed inadequate for effective data protection and without legal basis at EU and national level. Indeed, the current Europol Decision[18] does not cover tasks of mutual legal assistance on behalf of the EU such as the control of EU data prior to their possible communication to third countries.

On the other hand, in the current European framework, a possibility exists under the Eurojust Decision to assess TFTP requests at Eurojust level, and to have those requests validated and executed[19].

Taking into account the abovementioned lack of full powers of access of DPAs to all available information, the new task of confirmation to the data subjects that his/her rights have been respected under the TFTP2 Agreement[20] is not a task that the DPAs are in a position to fulfil. Also, DPAs cannot be appointed to a mere messaging task for UST assessments subsequent to EU data subjects' access or rectification requests.

Instead of such limited role of "UST mailbox", DPAs can only work in accordance with the standard set by article 28 Directive 95/46/EC, and provide independent compliance assessments. This implies that they can inform data subjects of the EU procedure that will be established under the TFTP2 Agreement and that could be followed for the exercise of rights, but without any guarantee of result and without declaration that this approach meets the applicable data protection requirements and principles.

---

15 Article 12.3 of the Agreement states

16 Article 12.2 refers to "independent oversight" but does not explain how this independence would be assessed in relation to the European standard set by article 28 of Directive 95/46/EC.

17 Reference to "ongoing monitoring" in article 12.3 "by an independent person appointed by the European Commission, with the modalities of the monitoring to be jointly coordinated by the Parties".

18 Council Decision of 6 April 2009 establishing the European Police Office (Europol), O.J., L 121/37

19 Based on the combined reading and application of the articles 9 quarter and 9 sexies of the Eurojust Decision; i.e. to include the national members of Belgium and Holland executing in their competence of national competent authority.

20 Included in Article 15.1 of the TFTP2 Agreement

## 4. Onward transfers – lack of any guarantees for the respect of several data protection principles and change from the current standard set by the Egmont principles for such transfers

Today, the principal mechanism for dealing with flows of financial intelligence is the Egmont Group, the international coordinating body of 106 FIUs, in accordance with the Egmont Statement of Principles of Information Exchange Best Practice[21] and using the Egmont Secure Web. Within the EU, FIUnet, an IT system linking most Member States' FIUs facilitates cooperation by allowing them to make enquiries and exchange certain information.

The WP29 and WPPJ are of the opinion that Egmont principles 11 and 12 offer a minimum benchmark of data protection that can and should be adequate and acceptable for the onward transfers under the TFTP2 Agreement. Egmont principle n° 11 addresses the requirement of purpose limitation. Egmont principle n° 12 provides the requirement of FIU consent for any further use (including onward transfers).

Even though the US Financial Intelligence Unit (FINCIN[22]), appears to be a part of the UST, and the Egmont Principles should therefore be deemed applicable to the UST, the WP29 and WPPJ fail to understand why the EU negotiating directives contain a lower level of protection than described in the Egmont principles n° 11 and 12.

The following data protection principles are not (identically or clearly) applied on onward transfers:

- the data retention limitation, including the retention mechanism of five years[23].
- the statement on the lack of involvement of data mining, manipulation or otherwise interconnection with other databases[24]
- the application of the purpose limitation principle / prohibition of incompatible use, as described in a stricter way in Egmont principle n° 11[25].

---

21 As published on http://www.egmontgroup.org/library/egmont-documents
*"11. Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.*
*12. The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information. "*

22 http://www.fincen.gov/

23 The current wording of the TFTP2 Agreement provides inadequate clarity and certainty to the question if and to what extent the data retention period is applicable to onward transfers in and outside the US

24 The wording of Article 5.3 of the TFTP2 Agreement contains the simple statement "The TFTP does not and shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering ". The correctness of this statement is difficult to verify. The statement is clearly not a firm commitment, nor an obligation that is applicable to onward transfers and other US or foreign programs, such as at the level of the Federal Bureau of Investigation that is partially a police and partially an intelligence service.

25 The (implicit) purposes linked to the tasks of the general categories of addressees for the ongoing transfers "*law enforcement, public security, or counter terrorism authorities in the United States, Member States, or third countries, or with Europol or Eurojust, or other appropriate international bodies, within the remit of their respective mandates"* in article 7 (b) of the TFTP2 Agreement are defined much wider than the purpose for the initial transfer/ request in article 4.2. (a) of the TFTP2 Agreement ("the purpose-of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing …). This is also much wider than the Egmont principle n° 11 for ongoing transfers ("used only for the specific purpose for which the information was sought or provided").

The consent of the authority that disclosed the information is a traditional precondition to limit incorrect or unlawful processing in onward transfers, and to protect the required data quality standards for antiterrorism and anti money laundering purposes. It can be found in Egmont principle n° 12 and should be already applicable to the UST. Instead, article 7 (d) of the TFTP2 Agreement provide possible exceptions if (the UST ?) deems that "*the sharing of the data is essential for the prevention of an immediate and serious threat to public security of a Party to this Agreement, a Member State, or a third country*"[26]. Such wide exception to the principle of consent is unknown under the existing Egmont principles and the necessity of such exception is not demonstrated.

## 5. Assessment of the "adequate" level of data protection

Article 8 of the TFTP2 Agreement contains the statement that "the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for purposes of tins Agreement". This statement is clearly inaccurate in light of current EU standards. As explained in our letter of 22 January 2010, "Traditionally, adequacy is assessed by a thorough comparison of the level of protection provided by a specific country or entity with EU standards." Since such an independent assessment has not yet taken place and is not foreseen in the (near) future, the level of protection offered by an agreement or the UST cannot be considered as adequate.

## 6. Joint Review

Taking into account the experiences with the US PNR agreement, the review mechanism should cover the whole term of the agreement (and should for instance specify that a review has to take place every year during the 5 year term of the agreement). There should also be a clear consequence (for instance the suspension or termination of the agreement) if no review is obtained, in case of misrepresentations or in case of repeated failure to comply with the basic data protection principles that is not remedied by the UST.

As set out in our letter of 22 January 2010, the effectiveness of the oversight powers of DPA's and the Joint Review stands or falls with the accessibility of all relevant information for all members of the review committee, including the representatives of the data protection authorities of the Member States.

However, DPAs are in particular concerned on the unknown modus operandi and in particular the limitations that might be required of the DPA's that will be called upon to be part of the joint review team[27]. In any event, DPAs can and should not be imposed to sign non disclosure agreements or meet other expectations that would appear to be conflicting with the requirements set out under article 28 of Directive 95/46/EC. In particular, the obligations to inform and be accountable to their national parliaments of the outstanding data protection issues under the TFTP2 agreement should be taken into account.

---

[26] "cases where the data is essential for the prevention of an immediate and serious threat to public security of a Party to this Agreement or of a third state"

[27] See also point 37 of the Opinion of the European Data Protection Supervisor of 22 June 2010 on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), published on www.edps.europa.eu

## 7. Lack of effective redress

A conflict appears between the articles 18.2 (redress mechanism) and 20.1 (no change in laws) of the TFTP2 agreement. The WP and the WPPJ understand that TFTP2 Agreement has no direct effect in the respective legal systems and that this agreement does not change in itself the respective legal systems of US, EU or national member states[28]. Today, the access and redress rights even differs from US agency to US agency and US law does not provide any rights to non-US citizens.

Since no rights for EU and non-EU citizens are created with direct effect under the TFTP2 Agreement, the WP29 and the WPPJ seriously question the effectiveness of the redress mechanism under US law as set out in article 18.2.

We trust that the aforementioned concerns will continue to receive due consideration by the European Parliament in its follow-up of the TFTP2 Agreement and remain at the Parliament's disposal for further information.

*Done in Brussels on 25 June 2010*

| | |
|---|---|
| Jacob Kohnstamm | Francesco Pizzetti |
| Chairman of the Art. 29 Working Party | Chairman of the Working Party on Police and Justice |

[28] See also points 11 and 32 of the Opinion of the European Data Protection Supervisor of 22 June 2010 on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II), published on www.edps.europa.eu