MEMO/10/258

Brussels, 15 June 2010

Terrorist Finance Tracking Programme – Comparison of Council Mandate with draft EU-US Agreement *(see IP/10/735)*

The present document provides a comparison between the Council Mandate (CM) providing directives to the European Commission for negotiating a Terrorist Finance Tracking Programme (TFTP) Agreement with the United States and the actual Draft Agreement (DA), initialled on 11 June 2010.

- COUNCIL MANDATE (CM): §1. The Agreement shall apply only to specific, designated providers of international financial payment messaging services ("Providers") as set out in its Annex for purposes of the Agreement;

  DRAFT AGREEMENT (DA): Article 3: "The Designated Providers shall be identified in the Annex to this Agreement and may be updated, as necessary, by exchange of diplomatic notes. Any amendments to the Annex shall be duly published in the Official Journal of the European Union."

- CM: §2. This Agreement shall provide that the request and the data, which is made available, shall take account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities. The request shall be narrowly tailored, proportionate and clearly substantiate the necessity of the requested data. Only the minimum amount of data, which is necessary for the purpose of the Agreement shall be requested by the United States Department of the Treasury.

  DA: Article 4(2): "The Request (together with any supplemental documents) shall:

  identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing;

  clearly substantiate the necessity of the data;

  be tailored as narrowly as possible in order to minimize the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses;"

- CM: The Annex should contain an exhaustive list of categories of data affected by the request. If need be the parties shall consult. The data shall then be made available to the United States Department of the Treasury;

  DA: *No exhaustive list in Annex but Europol will receive the full data categories (Article 4(2)(a))*

- CM: §3. The Agreement shall limit the processing of personal data contained in relevant financial payment messaging data exclusively to the prevention, detection, investigation or prosecution of terrorism and its financing as based on the approach of Article 1 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism and Article 1 of Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

  DA: Article 5(2): "Provided Data shall be processed exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing"

  Article 3: definition of terrorism and terrorist financing based on Council Framework Decision on Terrorism and Third Money Laundering Directive.

- CM: Each individual search shall be proportionate and demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing, and shall be logged, including such nexus to terrorism or its financing required to initiate the search.

  DA: Article 5(2): "All searches of Provided Data shall be based upon pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing."

  Article 5(3): "Each individual TFTP search of Provided Data shall be narrowly tailored, shall demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing, and shall be logged, including such nexus to terrorism or its financing required to initiate the search."

  ***See also Recital on proportionality as guiding principle of Agreement*.**

- CM: §4. The Agreement or its Annex shall provide that all transactions relating to the Single European Payment Area (SEPA) fall outside the scope of the data to be requested by or made available to the US Treasury Department, whichever system of financial messaging will be used;

  DA: Article 4(2): "The Request (together with any supplemental documents) shall: … not seek any data relating to the Single Euro Payments Area."

- CM: §5. The Agreement shall further provide that a public authority ("the Authority") shall be designated in the EU with the responsibility to receive requests from the United States Department of the Treasury.

  DA: Article 4(4) et seq: "Upon receipt of the copy, Europol shall verify as a matter of urgency whether the Request complies with the requirements of paragraph 2. Europol shall notify the Designated Provider that it has verified that the Request complies with the requirements of paragraph 2."

- CM: The request shall indicate as specifically as possible the financial payment messaging data.

  DA: Article 4(2): "The Request (together with any supplemental documents) shall: identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing."

- CM: On receipt of such requests, the Authority shall verify whether the substantiated request meets the requirements of the Agreement and, on the basis thereof, authorise or refuse the execution of the request.

  DA: Article 4(4) et seq

- CM: Following the authorisation by the Authority, the Provider shall be entitled to transfer, on the basis of a "push" system, the requested relevant financial payment messaging and related data.

  DA: Article 4(6): "The Designated Provider shall thereupon provide the data (i.e., on a "push basis") directly to the U.S. Treasury Department."

- CM: No other data shall be transferred, for technical or other reasons;

  DA: Article 6(2): "If it transpires that financial payment messaging data were transmitted which were not requested, the U.S. Treasury Department shall promptly and permanently delete such data and shall inform the relevant Designated Provider."

- CM: §6. The designated "Provider(s)", "the Authority", as well as the scope of the financial payment messaging and related data to be covered shall be further specified in the Agreement and/or its Annex;

  DA: Article 3: "The Designated Providers shall be identified in the Annex to this Agreement".

  Article 4 specifies that Europol is the public authority.

  Article 5(7): "Provided Data may include identifying information about the originator and/or recipient of a transaction, including name, account number, address, and national identification number."

- CM: §7. The Agreement shall ensure full respect for fundamental rights as enshrined in Article 6 of the Treaty on European Union, in particular the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union. It shall also ensure full respect for the principles of necessity and proportionality regarding the right for private and family life and the protection of personal data as set out in Article 8 of the European Convention on Human Rights and Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union;

  DA: Transparency, right of access, right of rectification, erasure and blocking are guaranteed by *Articles 14, 15 and 16*. Redress rights both administrative and judicial are guaranteed by *Article 18*. Recital states that proportionality is a guiding principle of the Agreement.

- CM: §8. The Agreement shall ensure, with regard to data transferred to the United States, rights of effective administrative and judicial redress on a non discriminatory basis regardless of nationality or residence for any person whose data are processed pursuant to this Agreement, in line with Article 47 of the Charter of Fundamental Rights of the European Union;

  DA: *Article 18* ensures non-discriminatory administrative redress, and rights of judicial redress for any person whose data are processed pursuant to the Agreement

- CM: §9. The Agreement shall contain safeguards and controls which ensure an adequate level of protection of personal data;

  DA: *Article 5* sets out detailed and legally binding safeguards and controls guarding against any wrongful processing of personal data under the Agreement.

- CM: §10. The Agreement shall ensure that personal data extracted from the TFTP database are kept for no longer than necessary for the specific investigation or prosecution for which they are accessed under the TFTP. As regards non-extracted data the Agreement shall establish a maximum storage period which shall be as short as possible, and provide for an ongoing and at least annual evaluation in order to identify and delete at the earliest possible stage all non-extracted data that are not necessary for the execution of the purposes referred to in the Agreement. The Agreement shall provide that this obligation to delete data within this period shall be binding on the United States also in case of termination or expiry of the Agreement;

  DA: Article 5(7): "Information extracted from Provided Data, including information shared under Article 7, shall be retained for no longer than necessary for specific investigations or prosecutions for which they are used."

  Article 6(4): Non-extracted data to be kept for no longer than 5 years. But NB also Articles 6(5) and 6(6) requiring assessment of whether the period should be reduced during lifetime of Agreement.

  Article 6(1): UST must undertake ongoing assessment to identify and delete data which are no longer necessary for purpose of Agreement. Article 12(4) states that data deletion obligations of the Agreement will continue to operate notwithstanding termination of the Agreement

- CM: §11. Onward transfer of information obtained through the TFTP under the Agreement shall be limited to law enforcement, public security, or counter terrorism authorities of US government agencies or of EU Member States and third countries or Europol or Eurojust, within the limits of their mandate. Onward transfer of personal data should be as limited as possible and subject to adequate safeguards comparable to those contained in the Agreement and will be subject to the prior consent of the competent authority of the Member State concerned, except in the 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. No personal data shall be shared other than that contained in specific lead information on identified individuals targeted by a terrorism investigation. Such information shall be transferred and used exclusively for the detection, prevention, or prosecution of terrorism or its financing. Each onward transfer shall be duly logged;

DA: *Article 7* sets out detailed limitations on onward transfer. Only data derived from individual searches pursuant to Article 5 may be the subject of onward transfer, such data are subject to a logging obligation, may only be shared with public authorities responsible for the fight against terrorism and exclusively for counter terrorism purposes. Where the UST is aware that the data are those of an EU citizen or resident, their onward transfer is broadly subject to the prior consent of the competent MS authorities; Onward transfer must be subject to a commitment by the receiving party to delete the data once no longer necessary for the particular investigation.

- CM: §12. The Agreement shall provide, with regard to data transferred to the United States, for

  1) the right of individuals to information relating to the processing of personal data;

  2) the right to access his/her personal data;

  3) to the rectification; and

  4) as appropriate erasure thereof;

  DA: Transparency, right of access, right of rectification, erasure and blocking are guaranteed by *Articles 14, 15 and 16*.

- CM: §13. The Agreement shall provide for the right of any person to obtain, following requests made at reasonable intervals, without constraint and without excessive delay or expense, at least a confirmation via his/her national data protection supervisory authority as to whether their rights as a data subject have been respected. It will clearly lay down the eventual limitations to the exercise of the right to access, rectification and erasure, that may be set out to safeguard the prevention, detection, investigation or prosecution of terrorism or its financing covered by this Agreement based on the principles of necessity and proportionality. Any refusal or restriction to access shall be set out in writing to the data subject, and information shall be provided on the means available for seeking redress in the United States. In all of these cases the data subject shall be advised that he/she may appeal to a judicial authority;

  DA: *Article 15* guarantees these rights of access and related procedural requirements.

- CM: §14. The Agreement shall prohibit that financial payment messaging data transferred to the United States Department of the Treasury are subject to data mining, manipulation or otherwise interconnected with other databases;

  DA: Article 5(3): "The TFTP does not and shall not involve data mining or any other type of algorithmic or automated profiling or computer filtering."

  Article 5(4): "…Provided Data shall not be interconnected with any other database; …Provided Data shall not be subject to any manipulation, alteration, or addition…"

- CM: §15. The Agreement shall provide for safeguards and controls regarding the protection of personal data made available pursuant to the Agreement, including the regular monitoring of such safeguards and controls. Such safeguards and controls shall be at least equivalent to those for US citizens under US domestic law and shall comprise those set out in the TFTP Representations. It shall reflect the standards set out in the Council of Europe Convention 108 of 28 January 1981;

DA: Article 5 sets out detailed and legally binding safeguards and controls guarding against any wrongful processing of personal data under the Agreement.

Article 12 confirms that the safeguards will continue to be subject to SWIFT scrutiny and inspection of independent auditors. In addition, the Commission may appoint an independent person who will monitor this oversight on a ongoing basis.

Article 13 sets out detailed provisions on the review of the Agreement by a Commission-led team of data protection, security and judicial experts.

- CM: §16. The Agreement shall provide that it does not derogate from the obligations of the United States and the Member States to make a mutual legal assistance request in order to use the data obtained as evidence in criminal proceedings.

  DA: Article 20(2): "Nothing in this Agreement shall derogate from existing obligations of the United States and Member States under the Agreement on Mutual Legal Assistance between the European Union and the United States of America of 25 June 2003 and the related bilateral mutual legal assistance instruments between the United States and Member States."

- CM: §17. The Agreement shall ensure that information, which is derived from the TFTP which may contribute to the prevention, detection, investigation or prosecution of terrorism or its financing by one or more European Union Member States shall be made available in the most expedient manner to competent authorities of the European Union Member States as well as to Europol and Eurojust, within the limits of their mandate. The Agreement shall further provide that appropriate searches of the TFTP database shall be carried out, under the same conditions and in the same manner as for US authorities, in response to a request made by the competent authorities of one or more European Union Member States, Europol or Eurojust and that these shall be provided with relevant extracted information under the conditions of the Agreement;

  DA: Article 9 states that the US will spontaneously provide information derived from the TFTP to competent authorities of MS and to Europol and Eurojust as appropriate where that information may be relevant to the fight against terrorism.

  Article 10 states that competent authorities of MS and Europol and Eurojust as appropriate, may request that UST carries out searches of the TFTP database in connection with an investigation of a person suspected of terrorism.

- CM: §18. The Agreement shall provide for a commitment of the US to cooperate with the EU if the EU decides to establish a database on European territory throughout the term of the Agreement so that the transfer of data can be more targeted in the future. It shall provide for a commitment of the US to cooperate with the EU if the EU decided to set up an EU TFTP throughout this time. It shall provide for a commitment that in the event of the European Union setting up an EU TFTP, competent US authorities shall agree to transfer relevant financial payment messaging data held in the United States of America to the competent EU authorities;

DA: *Article 11* provides for US cooperation in the event that the EU decides to establish a system equivalent to the TFTP leading to a more targeted transfer of data. It states that in this case, UST will provide assistance and support and that the Parties will assess how the Agreement needs to be altered to take account of such developments. It further provides for the transfer of messaging data between EU and US on a reciprocal basis in these circumstances.

- CM: §19. To avoid any risk that the envisaged Agreement could be seen as a precedent for data transfers in other areas, the Agreement shall state that it is specific to the fight against terrorism which represents a common EU-US interest and that the Agreement in no way constitutes a precedent for data transfers for any other purpose, for transfers of any other data or for any future EU-US data protection arrangements;

  DA: Recitals (third from last) state that the Agreement in no way constitutes a precedent for any other data sharing or data protection.

- CM: §20. The Agreement shall specify that the European Union shall, at its request, carry out regular and/or ad hoc reviews of the safeguards, controls and reciprocity provisions contained in the Agreement. Such reviews shall include access to TFTP systems to verify compliance with surrounding safeguards and controls. The reviews shall include a proportionality assessment of the retained data, based on the value of such data for the prevention, detection, investigation or prosecution of terrorism or its financing. The reviews shall include an assessment concerning the quantity of financial messages processed and the extent to which these data have been shared with other US agencies and/or third countries or Interpol. The review team shall include counter terrorism as well as independent data protection experts;

  DA: Atricle13 sets out detailed provisions on the Review of the Agreement. The Review will be led by the Commission with a team including independent data protection, security and judicial experts.

  Atricle13: "The review shall include a representative and random sample of searches in order to verify compliance with the safeguards and controls set out in this Agreement, as well as a proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing."

- CM: §21. The Agreement shall provide that the Commission will present periodical reports to the European Parliament and the Council on the functioning of the Agreement. The report shall indicate, in particular,

  1) the quantity of financial messages processed,

  2) an assessment of the effectiveness of the Agreement, including the suitability of the chosen instrument of transfer of information and the extent to which these data have been shared with other US agencies, public authorities of EU Member States or third countries, Interpol, Europol and Eurojust,

  3) the numbers of cases for which the information has been used for the prevention, detection, investigation or prosecution of terrorism or its financing and

  4) compliance with data protection obligations;

  §22. The report shall present an assessment of the implementation of the Agreement and of elements that would affect the compliance with the provisions of the Agreement;

DA: Article 13: "Following the review, the European Commission will present a report to the European Parliament and the Council on the functioning of the Agreement, including the areas mentioned above."

Article 13 specifies the areas which the Review will in particular address, namely "(a) the number of financial payment messages accessed, (b) the number of occasions on which leads have been shared with Member States, third countries, and Europol and Eurojust, (c) the implementation and effectiveness of the Agreement, including the suitability of the mechanism for the transfer of information, (d) cases in which the information has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing, and (e) compliance with data protection obligations specified in this Agreement."

- CM: §23. The Agreement shall provide for its termination by either party upon at least six (6) months written notice to the other party;

  §24. Moreover, the Agreement shall provide that the EU shall have the right to immediately terminate the Agreement or require suspension of the transfer of financial payment messaging data where safeguards on reciprocity or obligations are not complied with;

  DA: Article 21: "Either Party may terminate this Agreement at any time by notification through diplomatic channels. Termination shall take effect six (6) months from the date of receipt of such notification."

  Article 21: "Either Party may suspend the application of this Agreement with immediate effect, in the event of breach of the other Party's obligations under this Agreement, by notification through diplomatic channels."

- CM: §25. The Agreement shall specify that it in no way affects the data protection standards established by the relevant EU or national legislation applicable to the "Providers" nor limit the supervisory competence and powers of data protection authorities, which are competent for the supervision of data processing by the "Providers";

  DA: Recitals state that Designated Providers "are bound by generally applicable EU or national data protection rules, intended to protect individuals with regard to the processing of their personal data".

- CM: §26. The agreement shall expire no later than 5 years after its entry into force. One year before the aforementioned date the commission will undertake a study into an appropriate follow-up of the present agreement including the possible introduction of a EU mechanism.;

  DA: Article 23(2): The Agreement is for a period of 5 years renewable for one year periods unless otherwise terminated.

  Article 11(1): "During the course of this Agreement, the European Commission will carry out a study into the possible introduction of an equivalent EU system allowing for a more targeted transfer of data."

For more information

Homepage of Cecilia Malmström, Commissioner for Home Affairs:

http://ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_en.htm