Annex

This Annex considers specific issues thus far identified in respect of CRS and that should be taken into account so that the legitimate aim of combating fraud and tax evasion is carried out while ensuring that fundamental rights are duly respected. These points, however, do not represent an exhaustive list of the obligations under Directive 95/46.

1 Legal basis It is essential that any law and agreement including the CAA is accessible and foreseeable in accordance with the requirements of Article 8 ECHR, and that such instruments contain substantive provisions that implement (and not just merely refer to) Directive 95/46/EC and/or the national data protection law that implement the Directive.

It is also important that national procedures, providing for the involvement of respective Parliaments - and eventually DPAs - should be fully respected in order to create adequate, clear and foreseeable legal basis.

2 Purpose limitation In accordance with Article 6 of the Directive any Inter-State agreement should clearly identify the purposes for which data are collected and validly used. The wording on the purpose ("tax evasion"/"improvement of tax compliance") for example appears vague and insufficiently clear, allowing too much flexibility to the receiving authority. It is not clear whether such purposes include, for example, legal acts of tax evasion, illegal acts of tax evasion or (serious) financial crimes.

3 Necessity assessment under the proportionality principle Necessity and proportionality of data processing have been a main focus of the CJEU judgment in the Digital Rights Ireland case (see above). The WP29 is of the opinion that the CJEU ruling applies to automatic transfer of data and that therefore, in CRS it is necessary to demonstrably prove the necessity of the foreseen processing and that the required data are the minimum necessary for attaining the stated purpose[1].

4 Data retention Proportionality should also guide data retention. The WP29 reiterates that as a consequence of the CJEU judgment, national data retention laws and practices should ensure that any decision to retain personal data must be subject to appropriate differentiation, limitations or exceptions. The Court also highlighted that data retained outside EU, would prevent the full exercise of the control, explicitly required by Article 8(3) of the Charter, by an independent authority, an essential component of the protection of individuals with regard to the processing of personal data.

5 Transparency and fair processing Clear and appropriate information should leave data subjects in a position to understand what is happening to their personal data and how to exercise their rights, as foreseen by Articles 10 and 11 of the Directive. Any

[1] See WP's Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

restriction or exemption to those provisions must be duly limited and duly justified, and respect the strict criteria set forth in Article 13 of the Directive.

6 Data subjects' rights Due account should be taken for data subject's rights: any restriction or exemption to those rights must be duly justified and respect the strict criteria set forth by Article 13 of the Directive. Appropriate mechanisms to ensure easy exercise of their rights by the data subjects should be ensured.

7 Controllership Data controllers (and possible data processors) should be clearly identified. A correct allocation of controllership is indeed a crucial step in order to ensure compliance with the data protection principles and that data subjects are able to exercise their rights. (See WP's Opinion 1/2010 - WP169[2] - which outlines the concept of "data controller", its interaction with the notion of "data processor", and the implications in respect of allocation of responsibilities).

8 Onward transfers Data controllers involved in the exchange should ensure guarantees for onward transfers after the initial disclosure of data, in particular ensuring that the data are not used for general crime prosecution, without appropriate safeguards. In this regard, specific safeguards should be provided in the agreement governing the inter-state exchange, in order to ensure at least that the initial data controller is adequately informed of possible onward transfers, as well as the competent supervisory authority, and that data subjects can fully enforce their right of redress and access.

9 Security measures The processing in question would result in an exponential increase of the risks inherent in the processing of personal data in relation to the amount of information collected. Strict security measures should be adopted in particular to avoid accidental or unlawful destruction or any unauthorized disclosure or access and against any other unlawful form of processing as set forth by Article 17 of the Directive. In the light of the new framework emerging within the Proposed General Data Protection Regulation, the WP29 encourages the introduction of data breach notifications to the data subjects concerned and to DPAs. Moreover, the potential implications of the technical options that might be chosen in order to implement CRS, in particular in the light of the Court's decision of 8th April 2014 on the Data retention Directive, should be kept in mind.

10 Privacy Impact Assessment Given the scale of the proposed CRS and the potential large amount of persons that could be affected by same, together with the concerns identified in WP29's above preliminary findings, each Member State should consider to implement an agreed Privacy Impact Assessment aiming to ensure that the data protection safeguards are adequately addressed and a consistent standard is applied for the practical implementation of the CRS by all EU countries.

[2]The Opinion is available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf