ARTICLE 29 Data Protection Working Party

Brussels, 18 September 2014

Mr Pascal Saint-Amans
Director of Centre for Tax Policy and Administration
OECD
France
By e-mail: Pascal.SAINT-AMANS@oecd.org

Mr Achim Pross
Head of the International Co-operation and Tax Administration Division
OECD
France
By e-mail: achim.pross@oecd.org

Mr Michael Donohue
Head of Unit on Information Security and Privacy
OECD
France
By e-mail: michael.donohue@oecd.org

G20 Presidency
Department of the Prime Minister and Cabinet
Australia
By e-mail: G20info@pmc.gov.au

Mr Heinz Zourek
Director General of the EU Commission, DG TAXUD
Belgium
By e-mail: Heinz.Zourek@ec.europa.eu

Mr Martin Schulz
President of the European Parliament
Belgium
By e-mail: President@europarl.europa.eu

Mr Claude Moraes
Chairman of the Committee on Civil
Liberties, Justice and Home Affairs
European Parliament
Belgium
By e-mail: claude.moraes@europarl.europa.eu

Mr Stefano Sannino
Ambassador Extraordinary and Plenipotentiary
Permanent Representative of Italy
Presidency of the Council of the EU
Belgium
By e-mail: delegation.it@consilium.europa.eu

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and Union citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No MO59 02/34

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Subject: OECD Common Reporting Standard

Following a letter received from a member of the European Commission's Expert Group on taxation of savings (EUSD) in April 2014, and a further letter from the European Banking Federation (EBF) dated the 30 June 2014, which both raised data protection concerns in respect of "Standard for Automatic Exchange of Financial Account Information – Common Reporting Standard" (CRS) approved by the OECD Council on 15 July 2014[1], the Article 29 Working Party (WP29) has considered the Standard and intends to set out an initial evaluation of its impact on the protection of personal data.

The Standard - which is made up of an introductory part, a Model Competent Authority Agreement (CAA) and the Common Reporting Standard (CRS) containing the reporting and due diligence rules to be followed by financial institutions to identify reportable accounts - aims at setting out a global model for automatic inter-state exchange of information to address the issue of tax evasion.

The WP29 – which brings together representatives of data protection authorities of the European Union - is aware that mechanisms for automatic inter-state exchanges of personal data for tax purposes proposed by the OECD were also considered - at the Council of Europe level - by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD) in its Opinion, adopted on 4 June 2014[2].

The WP29 wishes to first point out that while the exchange of information is legitimately regarded as an essential tool in the fight against tax evasion, it is nevertheless necessary to ensure that such an objective of general interest is pursued with full respect for individuals' fundamental rights, in particular, the right to private life and the protection of personal data as required by European and international legal instruments (see *infra*).

1. Purpose of the current letter As a matter of urgency, due to the upcoming G20 Finance Ministers meeting (20-21 September 2014) that will consider CRS, the WP29, in this letter, wishes to make some preliminary remarks on a number of critical data protection issues raised by CRS. The WP29 may further consider an opinion on this topic, in particular after having engaged with relevant stakeholders.

---

[1]This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Published on http://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-financial-account-information-common-reporting-standard.pdf

[2]T-PD(2014)05, adopted on 4 June 2014, available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2014)05_En_Opinion%20tax%20(final).pdf

2. Previous findings of WP29 and further developments CRS draws extensively on the inter-governmental approach to implementing the US Foreign Account Tax Compliance Act (FATCA) which has already been considered by the WP29 in two letters to the European Commission, on 21 June 2012 and 1 October 2012[3]. In both letters, concerns were raised from the data protection perspective, which are also referred to here, where appropriate, in particular in respect of the need for an adequate legal basis for the transfer of personal data.

Recently, the WP29 investigated the differences in privacy and data protection in the various international financial cooperation agreements. The WP29 found considerable discrepancies in the international agreements established so far. For example, in the second TFTP agreement, more data protection guarantees are provided for than under both FATCA or CRS. The WP29 urges that appropriate data protection safeguards are provided in the different agreements at stake, thereby to ensure consistency and overall logic in the international legal framework.

3. Respect for privacy and data protection as basic, fundamental rights The WP29 shares the view expressed by the Opinion of T-PD[4], that it is essential that any exchange of data respects the rule of law and fundamental rights, enshrined by the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108/1981).

The WP29 highlights that Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) introduced by the Lisbon Treaty, establishes the principle that every individual has the right to the protection of personal data concerning them and renders the Charter of Fundamental Rights of the EU legally binding, which contains in particular Article 8 enshrining the protection of personal data as a fundamental right.

The WP29 also underlines that it is crucial that any operation having implications on data processing within the EU, including data transfer obligations, is carried out whilst ensuring compliance with the principles set forth by Directive 95/46 on the protection of individuals with regard to the processing of personal data, which apply to all sectors including the financial sector.

On more than one occasion, the WP29 has underlined the problems attached to agreements providing for repeated transfers of massive volume of personal data, including in Opinion WP114[5] where it stressed that such data transfers should be governed by appropriate agreements which should be legally binding and fully take into account all of the data protection safeguards under the Directive.

4. The adoption of a national or European law to approve inter-state automatic exchange of data must include substantive data protection safeguards The practical roll-out of CRS in Europe based on existing FATCA IT solutions currently lacks adequate data protection safeguards, notwithstanding the EU proposed to amend the Directive 2011/16/EU regarding mandatory automatic exchange of information in the field of taxation. This Directive – which could be considered as transposition of the US FATCA and CRS in EU law - so far falls short of data protection safeguards.

---

[3]See:http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf; and http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121001_letter_to_taxud_fatca_en.pdf

[4]See footnote 2.

[5]The Opinion is available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

CRS includes some data protection elements in the Model Competent Authority Agreement (CAA) to be used by states for exchanging information. The WP29 stresses that there are several different requirements which should be added because they are essential elements under existing European and international legal instruments, including international financial cooperation agreements. Also, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as reviewed in 2013, should be taken into account.

The WP29 recalls that Article 13.1(e) of the Directive 95/46 provides for exemptions and restrictions to the scope of some obligations and rights (information, right of access, publicizing processing operations) when necessary to safeguard *"an important economic or financial interest of a Member State or of the EU, including monetary, budgetary and taxation matters"*. However, such restrictions must be provided by appropriate legislative measures.

That said, the mere act of adopting a national law and/or European law (under Directive 2011/16/EU) or international tax agreements providing for the possibility to use an automatic exchange of personal data under systems such as FATCA or CRS, would not alone be enough to ensure adequate data protection. It is on the contrary necessary to provide in such laws for substantive provisions that put in place adequate data protection safeguards.

This is illustrated by the recent decision of 8 April 2014 of the Grand Chamber of the Court of Justice[6] (CJEU). In that judgment, the Court stressed the need for legislation to provide access for the competent national authorities to personal data and their subsequent use for purposes of prevention, detection or criminal prosecutions. The Court required objective criteria determining the limits for such operations, given the extent and seriousness of the interference with the fundamental rights as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

National legislators, authorities and institutions should be aware of this principle, which gives *a fortiori* for those processing operations designed to monitor behavior which does not have a criminal connotation.

5. Specific preliminary findings on data protection principles Against this background, the WP29 would like to draw attention to some specific issues thus far identified in respect of CRS and that should be adequately addressed to ensure that the legitimate aim of combating fraud and tax evasion is carried out with due respect for fundamental rights. These points, however, do not represent an exhaustive list of the obligations under the Directive. Please refer to the annex attached hereto.

Conclusions

This letter contains the WP29's initial views and concerns in respect of the possible implications on individuals' fundamental rights raised by automatic inter-state exchanges of personal data for tax purpose under both FATCA and CRS, also in view of a possible future opinion.

The Working Party would appreciate to be kept informed and will where necessary engage with the competent authorities in a common effort to assist in identifying the correct methods

[6]Cases C-293/12 and C-594/12, Digital Rights Ireland, Seitlinger a.o., published on http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293

to ensure that the legitimate objective to combat tax evasion is pursued through efficient mechanisms which do not expose individuals' rights to disproportionate interference.

Yours sincerely,
On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

CC: Mr Rolfjosef Hamacher, Axis Rechtsanwalt (Lawyer), Fachanwalt für Steuerrecht (Tax Lawyer), Germany.
By e-mail: hamacher@axis.de

CC: Mr Wim Mijs, Chief executive of the European Banking Federation
Send to: Mrs Georgieva Tsveta, personal assistant to the Chief Executive. Belgium
t.georgieva@ebf-fbe.eu

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