

ARTICLE 29 DATA PROTECTION WORKING PARTY



Brussels, 04 April 2013

Juan Fernando López Aguilar
Committee on Civil Liberties,
Justice and Home Affairs
European Parliament
Rue Wiertz 60
B-1047 Brussels
Belgium

Dear Mr. López Aguilar,

As you are aware the European Commission published on 6 February 2013 its proposal for a new Anti-Money Laundering/Counter Terrorist Financing (AML/CFT) Directive and a separate proposal for a Regulation on information accompanying transfers of funds, COM (2013) 44/2¹. Both documents have been submitted to the European Parliament and the Council, and intend to transpose the FATF recommendations.

On 14 February, representatives of the Working Party 29 (WP29), which is a forum of all EEA and EU data protection authorities, received a debriefing from both the Commission (DG MARKT), and the EDPS, who was informally consulted on the drafts in December 2012.

An initial analysis of the proposals shows that, while offering a clear improvement in some data protection areas, there are still several serious interpretation issues that will impact on privacy and data protection and deserve to be brought to the attention of the Council, the LIBE committee and the Commission.

The WP29 is concerned about the Directive applying the FATF recommendations without sufficiently taking into account the specific legal culture of the European Union where privacy and data protection are recognized as fundamental rights

¹ http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm#overview

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/policies/privacy/index_en.htm

Positive elements of the drafts

The impact assessment clearly includes data protection² as one of the 15 main policy options, and refers to WP29's previous Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing.

The Working Party 29 supports the approach not to include new data protection rules or principles in the draft Directive, taking into account the new legal framework on data protection that is currently being developed by the European Union.

Progress has been made regarding data retention mechanisms, where the risk of 'evergreen' data retention for AML/CFT purposes has been reduced in Article 39 of the proposed Directive. Furthermore the applicability of the right of access has been confirmed in recital 34 of the proposal.

However, some issues remain outstanding. The following are key concerns after an initial analysis of the proposals.

1. Function creep vs purpose limitation

The WP29 noted that the scope of the Directive has been extended to allow Suspicious Transaction Reports (STRs) to be used as a way to tackle tax fraud/tax evasion. This extended scope moves away the traditional purposes of processing operations set up to tackle money laundering and terrorist financing³. Whilst the proposal explains that the scope has been extended to be "*consistent with the approach for fighting against tax fraud and tax evasion*⁴ followed at international level in including a specific reference to tax crimes within the serious crimes which can be considered as predicate offences to money laundering," it is the view of WP29 that tax evasion, tax crime and serious tax crime are **not** synonyms. It is a.o. necessary to clarify the definition of tax crime⁵ for the financial institutions to effectively implement AML procedures. Differences in the member states appreciation of topics such as suspicious transactions, delayed payment of taxes, and between tax evasion and tax avoidance should be also taken in account before rolling out the AML/CFT measures in a blanket fashion.

The WP29 has already made clear⁶ that making purpose definition clear and meeting the purpose limitation principle are the only way to avoid the risk of function creep. The key concern is that, given the significant impact that AML/CFT laws may have

² Page 40 of the impact assessment

³ page 5 of the Draft Directive States : "The enhancement of the customer due diligence procedures for AML purposes will also assist the fight against tax fraud and tax evasion." See also recital 9, Art. 3(4)(f).

Article 31.3 provides that the FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering or associated predicate offences, potential terrorist financing or are required by national legislation or regulation. (...)

⁴ Commission Communication presenting an Action Plan to strengthen the fight against tax fraud and evasion, adopted by the Commission on 6 December 2012, COM(2012)722 final

⁵ The Directive contains the definition of "criminal activity, that includes "all offences, including tax crimes related to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months"

⁶ See page 7 of the Annex to the Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing

on a data subject, compliance policies and cooperation mechanisms should always follow a **strict and clear application of the purpose limitation principle** for both primary and onward transfers (such as via the STRs).

To include any form of tax crime⁷ as predicate offence for money laundering places any form of tax crime on the same level as the purposes such as the fight against terrorism and the prevention of money laundering. Although this measure is an option recommended by the FATF, the approach of the member states on the issue of tax crime is not uniform. Therefore introducing a general provision including "tax crimes" (although qualified on the basis of the sanction, see Art. 3(4)(f)) as predicate offence for money laundering constitutes a violation of both the purpose limitation and proportionality principles.

2. Lack of clarity

The WP29 believes that the proposal still lacks sufficient clarity which is likely to lead to disproportionate application (also known as 'goldplating') by those obligated under the Directive. This disparity undermines the approach to effective data protection.

2.1. 'Goldplating' the secrecy provision

The WP 29 understands that it is the Commission's view that the prohibition to disclose to the customer or to other third persons the fact that an STR has been transmitted or that a money laundering or terrorist financing investigation is being or may be carried out (so called "tipping off" provision) relates only to STRs. For example if a data subject wanted to discover if an STR had been filed by the obliged entity with an FIU, the obliged entity would not be able to confirm or deny this fact.

However, some WP29 members have direct experience that demonstrates that some national regulators and obliged entities interpret this aspect very differently, for example by 'goldplating' the tipping off provisions to such a degree that they not only include STRs but also Know Your Customer (KYC) and Customer Due Diligence (CDD) information which are used for customer profiling operations for AML/CFT purposes. Such interpretations have a serious impact on the ability of the data subjects to exercise their access rights.

Case law on this issue has already expressed the view that it is an essential element of privacy protection for the law to "*indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*".⁸

At present, the current proposal leaves the risk of arbitrary interpretation and blanket fashion application by both obliged entities and national regulators.

⁷

In some countries tax evasion is a crime. In some member states it is not illegal.

⁸ ECHR, 26 march 1987, *Leander vs. Sweden*, § 51 and ECHR, 4 may 2000, *Rotaru*, § 52:

To solve this issue the Directive should set out more clearly that to achieve compliance national regulators and obliged entities should always make sure that the prohibition of tipping off has a clearly limited scope, thus limiting the data subject's access and rectification rights only in proportion to the aim pursued.

Recommendation: The Working party is of the opinion that the current interpretation of AML/CFT laws in relation to the prohibition of tipping off is causing arbitrary limitations to the rights of access and rectification in the member states. It recommends the European Union to specify more clearly in the AML/CFT Directive what processing operations (such as KYC or CDD operations) do not fall under the prohibition of tipping off, and to oblige national regulators and the industry to amend the matter accordingly.

2.2. Defining “important public interest”

Recital 32 of the proposed directive refers to the fact that tackling AML/CFT is an “important public interest ground”. When reviewing this within the meaning of article 26(1)(d) of Directive 95/46/EC, a recital statement is not enough to provide an adequate legal basis to legitimise transfers of personal data for AML/CFT purposes to third countries without an adequate level of data protection.

The WP29 recalls that, in its opinion WP 114, it has already set out the following advice when interpreting the provisions under Article 26(1): the use of derogations under article 26(1) should be “strictly interpreted” and although “there will be cases where mass or repeated transfers can legitimately be carried out on the basis of Article 26(1)”, when certain conditions are met, “transfers of personal data which might be qualified as repeated (...) or structural should, where possible, and precisely because of these characteristics of importance, be carried out within a specific legal framework(...)” In short, the application of article 26(1)(d) in this context should be transposed in the AML/CFT laws of the Member States. For this purpose there should be a substantial provision in the text of the Directive and not only a recital.

Further to the above point on onward transfers, the WP29 also believes that BCRs, contractual clauses nor Safe harbor mechanism are (in of themselves) not appropriate safeguards for the data subject because of the international mandatory law status of the reporting obligations, CDD and KYC obligations and processing operations. However, suggestions of the contrary keep on popping up, such as in the recent FATF/GAFI⁹ questionnaire.

Recommendation: The WP 29 encourages the European Union to set out more clearly the conditions to legitimise transfers of personal data for AML/CFT purposes to third countries without an adequate level of data protection. Member states should be obliged to deal more clearly in their national AML/CFT laws with the topic of transfers of personal data for AML/CFT purposes to third countries without an adequate level of data protection, by specifying what important public interests exist for the transfer of which data to which country, and what guarantees are made available to enable effective data protection.

⁹ The recent GAFI Questionnaire refers to “safe harbour or other specific bilateral (or multilateral) arrangements to permit the transfer of information to other countries, in particular for AML/CFT purposes”.

2.3. Transparency

WP29 understands that, to some extent, AML/CFT operations will necessarily be confidential. However the WP29 has already recommended the obliged entities to provide easy to use public data protection policies¹⁰ which are as transparent as far as possible on AML/CFT processing operations. This is especially the case for the KYC and the CDD obligations so that data subjects can exercise their right of access and rectification.

Recommendation: The WP29 recalls its recommendation for the obliged entities to use public data protection policies related to AML/CFT.

2.4. Data minimisation, necessity and proportionality of CDD and KYC

The wording of the Annex II (simplified customer due diligence) is insufficiently clear.

The type of data that could be processed under CDD obligations is very unclear. This could be clarified following a privacy impact assessment and its details could be put on face of the legislation. Alternatively, the Directive could oblige industry and/or financial regulators to produce guidance that illustrates the necessity for specific personal data to be processed, what types of data and what accompanied documents should (and should not)² be collected. Any formal instruction for systematic and blanket collection of documents to identify the source of funds for all clients and beneficial owners is contrary to the risk-based approach of the directive (art.11 par.2) and the data minimization obligation.

The WP29 recalls that there is a requirement to obtain clarity and foreseeability of the AML and CFT laws embedded in article 8 ECHR. According to the case-law of the ECHR¹¹, *“the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life”*. This case-law has a multi-layered impact on the CDD obligation.

If personal sensitive data (as defined in Article 8.1 or 8.5. of Directive 95/46/EC) are to be processed, it should be justified on a case by case basis¹² and be strictly necessary for the fulfilment of the obligations under the AML/CFT Directive. Also, appropriate safeguards should be in place for every processing of sensitive data or profiling operation and should be provided for in domestic law.

The current CDD obligations (articles 9, 10 and 11 of the draft Directive) contain a blanket profiling obligation for all clients (customers). The wording in articles 10 (e) and 38 of the draft AML/CFT Directive is very vague¹³.

¹⁰ See recommendation n° 12 in the annex to the Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing

¹¹ See the case law of the ECHR, a.o. ECHR, 26 march 1987, Leander vs. Sweden, § 51

¹² Council of Europe, point 3.11 of the recommendation CM/Rec(2010)13. The explanatory memorandum refers to article 6 of Convention 108.

¹³ Article 10 (e): “where there is suspicion...”

Recommendation: The WP29 calls for more specific modalities and/or appropriate safeguards to be added every profiling operation, such as CDD.

3. Continued and improved cooperation amongst different AML and CFT stakeholders

The Working Party 29 refers to its previous opinion 14/2011 of 13 June 2011¹⁴, that contained a recommendation to ensure legal certainty at EU level by encouraging continued and improved cooperation amongst the different stakeholders such as DPAs, FIUs and financial regulators.

While the proposal does contain in its articles 46 to 54 provisions for cooperation within the field of AML/CFT, it does not refer to any provisions that encourage cooperation in the field of data protection.

Several indications show that there is a clear need to recommend such cooperation, in accordance with the national laws.

- The WP 29 recalls that structural cooperation is customary in some member states based on article 20 Directive 95/46/EC for processing operations that are likely to present specific risks to the rights and freedoms of data subjects such as CDD obligations and the prohibition of tipping off. An obligation of privacy impact assessment for the member states is mentioned in article 33 of the draft Regulation.
- WP29 recalls its proposal to the Commission to develop a standard MOU, to ensure that MOUs always cover the data protection safeguards¹⁵.
- Recently, WP29 found that the handing of GAFI/FATF questionnaires¹⁶ in the member states was dealt with in the most diverse way in the different member states. In some countries, there was no consultation with DPAs whilst others were given the opportunity to provide feedback on the application of privacy and data protection. Some DPAs decided not to reply to such questionnaires, taking into account the different priorities of the FATF/GAFI, not embedded in the legal culture of the European Union where privacy and data protection are recognized as fundamental rights.

Recommendation: The WP29 recommends adding in the draft Directive an encouragement to improve the cooperation amongst the different stakeholders such as DPAs, FIUs and financial regulators in the field of data protection. This may either be a reference to the requirement of prior checking as laid down in article 20 of Directive 95/46/EC, or a reference to the requirement of a privacy impact assessment as mentioned in article 33 of the draft Regulation.

¹⁴ Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing

¹⁵ See point 3 page 10 of the annex to the Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing

¹⁶ FATF/GAFI questionnaires to delegations on the interaction between AML/CFT requirements and data protection and privacy rules

Conclusion

The WP 29 welcomes the recommendation in the ongoing discussion of the European Parliament's Special committee on organised crime, corruption and money laundering to provide efficient combating of money laundering by (a.o.) developing “*an effective regulatory framework that takes into account the interaction between anti-money laundering provisions and those relating to the protection and processing of personal data, and its correlation with identity fraud*”.¹⁷ The WP 29 supports any action that takes into account the interaction between anti-money laundering provisions and those relating to the protection and processing of personal data.

The WP 29 is of the opinion that the current draft does not meet this aim as some key data protection issues have not been fully resolved. Despite the current good intentions of the European Commission to take into account privacy and data protection by adding general references to data protection elements in recitals (and in one article the data protection Directive), WP29 found the Directive is still plagued by interpretation and goldplating issues that exist at national level.

A clearer wording in the Directive on problematic key areas or a more uniform legal instrument in this area is an additional option that may be considered to deal with the current lack of clarity and arbitrary limitations of the draft directive and the major differences (“goldplating”) in the national AML/CFT laws.

Since the scope of the Directive has been extended to include tax crime and tax evasion, justifying this is as an “*associated predicate offence*”, the WP29 has significant concern that this could be in breach of the principles of purpose limitation and proportionality.

The Directive does not deal adequately with the current lack of clarity and arbitrary limitations of the national AML/CFT laws, which is a clear data protection issue under existing case law (article 8 ECHR). Essential AML/CFT obligations, such as the prohibition of tipping off, the lack of clarity and guarantees for profiling (CDD) obligations, and the lack of national laws that clearly confirm the principle and conditions for obliged entities to use the important public interest ground to legitimise international transfers to group entities for specific AML/CFT data to specific countries without adequate data protection are some examples. Safeguards and clarity for such AML/CFT obligations are essential to obtain legitimacy in the area of data protection.

Effective cooperation between the different stakeholders in the area of data protection is not encouraged.

¹⁷ See page 10 point (j) of the working document III of the rapporteur S. IACOLINO, published on http://www.europarl.europa.eu/meetdocs/2009_2014/organes/crim/crim_20130218_1530.htm

The WP29 confirms its willingness to continue to cooperate with the different EU stakeholders (Commission, Parliament, Council, FIU Platform, Platform of financial regulators) in order to achieve both effective data protection and an effective countermeasures against money laundering and terrorism.

Yours sincerely

For the Working Party

The Chairman
Jacob KOHNSTAMM

cc: Ambassador Rory Montgomery, Permanent Representative
Mr Ruairí Gogan, Civil Law Matters, Fundamental Rights, Data Protection,
EAPO
Mr Jonathan Faull, Director General for "Internal Market and Services"