ANNEX

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT RECOMMENDATIONS

TABLE OF CONTENTS

34. *Uniformity and development of access schemes via DPAs*
35. *Resources for independent guidance by DPAs*
36. *Development of the principle of fair en legitimate processing*
37. *Only process sensitive data if suitable safeguards are specified in AML /CFT laws*
38. *Measures to prevent and remedy cases of identity theft*
39. *Political solutions to bind authorities in countries without adequate data protection*
40. *Method to establish adequate data protection*
41. *Replacement of the Council Decision of 17 October 2000 (exchange of data between EU FIUs)*
42. *Standard FIU request forms*
43. *Modalities of exchange via MOU's to FIUs in countries without adequate data protection*
44. *Application of the principle of availability in accordance with data protection principles*

1. Introduction

1.1. History

In early 2009, it was decided by the Working Party 29 (hereafter WP29) that the financial matters subgroup would identify the issues posed by the Anti-Money Laundering legislation, taking account the work of DG MARKT[1] since 2008 on money laundering obligations for reporting entities and Financial Intelligence Units ("FIUs") and data protection requirements[2].

1.2. Consultation process

Since June 2009, several meetings have been organized in the presence of EC DG MARKT, EC DG Justice and a limited number of representatives of national financial regulators and national Financial Intelligence Units (FIUs) to discuss the main issues and obligations in the area of AML (Anti-Money laundering) and CFT (Combating the Financing of Terrorism). The rapporteur also participated at several meetings of the FIU platform to discuss the consultation process.

1.3. Context

The entry into force of the Lisbon Treaty on 1 December 2009 has had a significant impact on the EU legal framework on privacy and data protection. Its impact on the processing operations for the purposes of AML and CFT is still being assessed. In the Stockholm program, an action plan was established that intends to amend the existing (previously "third pillar") prior to the adoption of the Lisbon Treaty.

1.4. Motivation of the need for practical and broad recommendations on privacy and data protection compliance by the WP29 in the area of AML and CFT processing operations

From the abovementioned discussions, it became clear by mid 2009 that there was a need for practical and broad guidance from the WP29 in the area of AML and CFT processing operations. It quickly became apparent that this requirement goes beyond the mere application of (amongst others) the EU Directives 1995/46/EC[3] and 2005/60/EC, in relation to the processing of personal data at the FIU level particularly when discussing the different issues linked to international transfers of data for AML and CFT purposes under the TFTP2 Agreement and the Egmont Group of FIUs[4].

More specifically, the need for practical recommendations from the WP29 is illustrated by the following issues that were either in published reports[5] or brought to the attention of the subgroup:

---

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

2 The Belgian DPA, started to work on this issue as rapporteur and submitted (in June and December 2009) an internal discussion paper that contained an overview of the main obligations and a description of problems and areas of tension between data protection and anti money laundering regulations.

3 Hereafter the "DP Directive"

4 http://www.egmontgroup.org/

5 page 15 of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

- On 30 June 2009, the European Commission published a working paper that referred to the added value of EU level clarification or guidance in the area of data protection[6].
- The fourth and ninth FATF recommendations on "secrecy laws"[7], and CDD and record keeping currently have a confusing approach on privacy and data protection. The FATF approach so far appears to be mainly about exploring possible exemptions from data protection requirements in order to meet the FATF obligations, rather than to approach privacy and data protection in a positive way; i.e. as an established human right of a democratic society, as understood in the European Economic Area and beyond.
- However, in early 2011, the FATF working group on evaluations and implementation investigated data protection issues. One of the proposals was to launch a high-level statement to seek a correct balance between fundamental rights of privacy and data protection and AML and CFT obligations. However, no formal consultation with data protection authorities such as the EU DPAs[8] and/or WP29 was initiated, even though FATF is, amongst other things, concerned to develop practical proposals that address the need to exchange information for AML and CFT purposes in a multinational context (KYC, CDD and STR obligations), and to manage perceived conflicts between AML/CFT and data protection obligations.
- Informal contacts were established in the financial matters subgroup and the FIU platform with a limited number of EU financial regulators and EU FIUs. It became apparent that, in a number of member states, a lack of (calls for) (in)formal assessments and collaboration amongst national financial regulators, financial supervisors, FIUs and DPAs exist, despite the existence of article 20 of Directive 95/46/EC and the work of the European Commission. In two cases the rapporteur found that the supervising authorities apparently ignored even their mutual existence and competence altogether. This may be due to a simple lack of awareness of competent authorities in member states and/or the fragmentation of supervision tasks and supervisory powers between different authorities in member states that could be addressed via recommendations.
- Insofar as EU AML/CFT laws could have a significant impact on the rights of individuals, WP29 regrets that such regulations do not include express references to important data protection obligations and do not provide the necessary clarity on other areas that are essential for effective data protection. Such gaps and vagueness leave a discretionary margin of interpretation to the private sector (hereafter also referred to as "institutions" and "reporting entities") to properly identify their data protection duties in the context of AML/CFT activities. This creates legal uncertainty and thus can lead to an unbalanced view on the legality and legitimacy of these processing operations.
- A relatively high lack inconsistency and imbalance in the application of the regulation in both areas (AML/CFT and data protection[9]) was also reported both by the European Commission and representatives of the institutions. The European

---

6 page 15 n° 39 of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

7 "Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF recommendations".

8 However, the FATF was contacted by the subgroup financial matters on 6 December 2010 to start a balanced discussion on the main concerns of the FATF.

9 In its document of 1 December 2010, the FATF working group on evaluations and implementation emphasizes strongly the lack of consistent application of data protection laws, while not addressing the similar lack in the area of AML and CFT laws, and the need for a balanced view through informal and formal concertation between competent authorities in both areas.

Commission referred to the possibility for regulators to be more stringent than the minimum harmonization requirements of the Directives[10]. Institutions reported to the subgroup the phenomenon of "goldplating"[11] of AML-CFT obligations[12]. Examples that were reported included advanced data sharing and consolidation at group level, 'evergreen' data retention schemes (see below).

- Institutions and FIUs repeatedly referred to the difficulty in interpreting data protection rules correctly in the context of AML/CFT obligations, a.o. due to the open nature of data protection norms.
- The different legal language used in both regulatory areas, often using sector specific abbreviations (such as KYC[13], CDD[14], STR[15] etc) and definitions in the different regulatory areas, hinder effective consultation and cooperation. In some cases similar but different wording is used to describe similar situations such as for the requirements for data sharing ("equivalent"[16] vs. "adequate" protection), "customer due diligence" and "risk assessment" or "fraud management" operations and obligations vs. "data protection opinions" that often refer to (financial) "profiling"[17] or "blacklisting".
- Several AML /CFT regulations interpret traditional EU data protection principles differently and sometimes incorrectly as intended by the Directive 95/46/EC. One example is the use of the wording "adequate" data protection in the TFTP2 Agreement. Others include the incorrect interpretation of the EU data protection laws by the FATF that appears in the statement that the specific consent of national DPAs would be required prior to transferring information[18], and the assumption that the application of the safe harbour scheme and data consolidation would be able "to address the obstacles to cross-border exchanges".
- Another finding is that new AML / CFT principles[19] introduced actually defend the opposite of traditional data protection obligations and principles. Furthermore, correct reference to the legal framework on data protection is sometimes completely or partially[20] ignored. Of course, such reference cannot replace proper implementation of and, attention to, the impact of data protection principles and obligations.
- Finally, DPAs continue to be contacted by citizens that report perceived privacy and/or data protection problems even when such perceptions are not always justified. Often, questions and concerns are caused by the perception of "insensitive" (sic)

---

10 Page 4 n° 6 of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

11 In the following meaning: To go further than is strictly required by the EU AML/CFT regulations. This process may easily ignore the impact on privacy and compliance with data protection principles and obligations in the process if no formal prior checking is provided by the national financial supervisor.

12 After transforming the AML/CFT directive into national law the German legislator added a regulation in Art. 25 g of the German Banking Act (KWG). The regulation contains stricter ("goldplated") requirements for preventative measures that must be met by all companies of a group to ensure compliance with the German money laundering act. The German regulator BaFin has published a formal interpretation of Art. 25 g KWG which is binding for the reporting entities (circular 17/2009 (GW)).

13 Know Your Customer

14 Customer Due Diligence

15 Suspicious transaction report (from institution to FIu)

16 Article 16.1 of the AML/CFT Directive creates a proper standard for "requirements (…) equivalent to those laid down in this (the AML/CFT) Directive)" , which may apply to third countries

17 See for instance page 2 of WP 164 "Contribution of the Article 29 Working Party to the public consultation of DG MARKT on the report of the Expert Group on Credit Histories, adopted on 1 December 2009) that insisted on the "provision of precise and specific guarantees with regard to data protection rules."

18 See however articles 25 and 26 of the DP Directive.

19 See the principle of availability mentioned in the recommendations

20 See for instance the limited attention in recital 33 of Directive 2005/60/EC to the rules of transfer of personal data

questionnaires sent by institutions, as illustrated by some press releases[21] in member states that introduced reinforced KYC and CDD obligations. Such concerns raise questions about the clarity of information practices of institutions and the need for the clarity and foreseeability of the AML and CFT laws and/or general policies[22] for the general public.

1.5. **Overview of the main aim and data protection issues**

In addition to the above elements, WP29 finds that the issues with the operations for AML/CFT purposes should be addressed through specific recommendations that aim to ensure a **more balanced interpretation and application of both regulatory areas within the EU[23].**

Main issues of concern are :

- there is a requirement for transparency and foreseeability of the AML/CFT laws and external and internal AML/CFT policies of financial regulators and institutions, and of visible financial measures that are perceived by the public as privacy infringements (i.e. KYC and CDD; questionnaires and document requests, blocking of assets, transactions, feedback etc);
- there is a requirement for purpose definition and meeting the purpose limitation principle to avoid the risk of function creep in these laws and policies;
- the possible "fora" for (in)formal discussion between DPAs, financial regulators, financial supervisors and other stakeholders are often not developed;
- the use of profiling techniques under CDD obligations in both AML/CFT and data protection areas often operate without a clear legal basis for the specific modalities and/or appropriate safeguards for every CDD operation;
- there is a requirement to meet the proportionality, data minimization principles and data retention periods/mechanisms (in order to avoid the risk of 'evergreen' data retention). I.E. AML/CFT processing regulations often lack clear limitation mechanisms[24];
- the roles and responsibilities of the data controller (FIUs, institutions) and data processors are often over-looked unmentioned, even when considering the development of the (outsourcing) service industry in the area of AML/CFT processing services;
- concerns exist regarding data quality and fair processing of identifying and profiling data;
- the impact of the legal protection of sensitive data is often overlooked;
- a lack of "prior assessment" exists of AML risk management measures that are encouraged and developed by (national) financial regulators, financial supervisors and institutions. For example no prior assessment was undertaken before the introduction of global AML risk management obligations in at least 15 EU member states[25].

---

21 See for instance the French press of 17 March 2010 (http://www.20minutes.fr/article/391636/France-Des-particuliers-se-sont-plaints-a-la-Cnil-de-questionnaires-de-banques-indiscrets.php)

22 See in this light also the Council of Europe's work on profiling.

23 Instead of a total exemption of AML and CFT operations from the protection by mandatory data protection laws within the EU, a stance defended by some stakeholders such as the FATF.

24 Under Directive 2005/60/EC and (for FIUs) articles 4, 5 and 9 of Council Framework Decision 2008/977/JHA

25 Page 5 n° 7 of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

- a lack of a balanced approach of both regulatory areas[26];
- the implementation of the requirement for adequate data protection in the area of AML/CFT processing operations (in case of transfers of personal data from the EU to third countries such as for intra-group transfers).

2. Recommendations

Legal basis and legitimacy – Application of the DP Directive, impact of Lisbon Treaty and decisions of national constitutional courts

1. It is not sufficient that processing operations for AML/CFT purposes are simply based on the large margin of interpretation by institutions or on an exemption to data protection obligations, to provide an adequate legal basis or another legitimate ground for processing (as defined by the DP Directive and article 8 ECHR). For AML/CFT authorities and institutions to legitimately process personal data, WP29 recommends to work **only on a clear legal basis under national or EU law[27]** as defined by article 8 ECHR. This requires either "a legal obligation to which the data controller is subject"[28], or "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed"[29]. Contrary to the current assessment by some institutions[30], WP29 is of the opinion that legitimacy for AML/CFT processing on other grounds such as **"legitimate interest" or "consent of the data subject"** faces serious difficulties. The grounds of "legitimate interest" relies mainly on a non-transparent intra-bank assessment of the need for processing that appears to be in conflict with the requirement of foreseeability of the law under article 8 ECHR. "(Explicit) consent" is more often than not used as the default[31] , but is an incorrect application of the definition of consent[32] in line with the DP Directive. The ground of "freely given consent" requires that the data subject has the power to withdraw his/her consent. Therefore it would be impossible to argue that consent is freely given to carry out profiling obligations (CDD) as a result of complying with national legal safeguards as the data subject has no option to opt out of such obligations.

2. AML/CFT laws, and their accompanying instruments and clarifications (guidance by financial regulators, best practices etc) should always describe in a balanced way the AML/CFT and DP rights and obligations[33]. Financial regulators, financial supervisors, FIUs and reporting entities/institutions should avoid "goldplating" (see above) in the interpretation of AML/CFT laws by and instead, **balance AML/CFT laws and with DPm obligations and provide balanced guidance** by carefully defining the exact scope and necessity of the AML/CFT tasks and obligations, and to add specific data privacy assessments, guarantees and requirements, whilst at the same time, referring to the main data protection obligations

---

26 One example is getting the right balance between the application of access and rectification rights and the prohibition of tipping off through existing, access, ratification and mediation procedures in national data protection laws that are often ignored, forgotten about or overlooked by financial regulators and financial supervisors

27 This may differ from instruments outside of the EU such as under FATF or BIS recommendations or guidance

28 Article 7 (c) of the DP Directive

29 Article 7 (e) of the DP Directive

30 See annex 7 (page 58) of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

31 See the institutions recourse to standard consent clauses included in the banks' general terms and conditions referred to in the last paragraph of annex 7 (page 58) of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

32 See the elements freely given, specific and informed in article 2 (h) of the DP Directive.

33 Corresponds with conclusion n° 10 of the briefing paper

and principles that correspond to the specific data privacy assessments, guarantees and requirements[34]. This recommendation for balanced laws and guidance applies to different internal / external tasks and obligations of different entities such as reporting entities[35] (institutions), FIUs[36] and financial supervisors (supervision role compared to the supervision tasks of DPAs)[37] .

3. Now would be a good opportunity for **a review of all current and proposed AML/CFT laws and practices at EU and domestic level**, in the light of the compliance with the current data protection and human rights framework[38] at EU and national level [39]. This review should assess:

- **Independent assessment** (or lack thereof) and effective oversight over AML/CFT processing operations[40] or AML/CFT laws (particularly by regulators and supervisors) should be considered, particularly any lack of essential guarantees to effectively strike a balance between the instruments to achieve this aim.
- AML/CFT laws at EU and national level[41] should always be **interpreted** in a balanced way, in accordance with the (constitutional) requirements[42] of privacy and data protection at EU and (as the case may be) national level;
- Subsequently, reporting entities should also implement existing AML/CFT polices in such a way that they comply with data protection requirements. In case they have not already done so, they should conduct a **re-assessment program for corporate compliance policies**[43]. This should address the current issues caused by the lack of compliance of existing instruments with data protection principles.

---

34 Example: guidance should refer to a data retentions scheme, and explain this requirement is imposed in execution of the proportionality and data minimization principles.

35 Relevant obligations are the (boundaries of) the prohibition of tipping off, the KYC and CDD obligations, the reporting obligations (STR) and data retention schemes, staff training programs under article 35 Directive 2005/60/EC should also include privacy responsibilities and risks in the context of AML / CFT processing

36 Such as the feedback mechanism, especially during ongoing investigations, data retention schemes,…

37 The combined application of article 37 of Directive 2005/60/EC (powers and tasks of financial supervisors) and article 28 Directive 95/46/EC (powers and tasks of DPAs) raises questions of role description, efficiency and balanced interests. Conflicts between positions under both supervision schemes and gaps in supervision should be avoided.

38 See the relevant conclusions and recommendations n° 1, 4, 5 10, 13 and 15 of the briefing paper of the European Parliament, titled "Current challenges regarding respect of human rights in the fight against terrorism" that are partially applied and further developed in these recommendations (Dated 28 April 2010, Ref. EXPO/B/DROI/2009/27). This paper recalls that, in the post Lisbon treaty era, the EU and its member states have reaffirmed their commitment to human rights.

39 There are clear national precedents that affirm different possibilities for intervention at national level against implementation of European law. The examples vary from member state to member state. See the German Solange Judgments of 1974 and 1986 that reserve the right to question the primacy of EU law in case the European law is incapable of upholding fundamental constitutional principles at national level. However, it is more likely that the EU law part of the legislation may be left unchallenged, while the portion of the national implementation law may be nullified. See the German Decision of 2 March 2010 in the data retention file published in German on http://www.bundesverfassungsgericht.de. See also, the Romanian Judgment of 8 October 2009 published on http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html. In the last case, a lack of precision in the national provision was criticized

40 See conclusion n° 13 of the briefing paper.

41 Including but not limited to the AML / CFT Directive and the Council Framework Decision and their local transpositions

42 a.o. the required level of transparency, precision and proportionality of the EU and national laws by the decisions of the ECHR, the Court of Justice and the constitutional courts.

43 Corresponds with conclusion n° 10 of the briefing paper

- In its Opinion of 1 December 2009[44], WP 29 already referred to the need to ensure the consistency of AML/CFT data processing operations (a.o. under Directive 2005/60/EC) with the principles and legislation on data protection. In this opinion, the WP29 called for **"*a reflection* on 'a comprehensive and consistent data protection framework covering all areas of EU competence"**[45], while leaving a margin of flexibility for specific sectors such as AML-CFT.
- More specifically, for the AML-CFT sector, WP 29 now recommends (on a non-exhaustive basis) to identify the relevant regulatory measures (hard law and soft law measures; EU and international measures) according to which the processing operations take place (that is, the legal sources of the data flows); and to intervene on such measures, depending on the legal source of the AML/CFT obligation.
- As it has been mentioned above, the Lisbon Treaty is having a significant impact on the Community data protection legal framework. Data protection has been recognised to be an autonomous, fundamental right, which should therefore be integrated in any legal instrument dealing with the processing of personal information. The Article 29 Working Party believes that this is the appropriate moment to make an exhaustive assessment of the existing AML/CFT legal framework from the data protection perspective, in order to identify possible gaps or vagueness that could make it difficult to apply this legislation in conformity with data protection requirements; and to act upon it. A comprehensive approach recommends not only assessing Directives 2005/60/EC and 2006/70/EC, but also the relevant legal instruments adopted under the former third pillar, such as the Council decision 2000/642/JHA.
- With reference to the exchange of personal data according to Memoranda of Understanding (MoU) from a FIU located in the EU to a third country FIU, the WP 29 proposes the EU Commission, in cooperation with the FIU Platform, develop a standard MOU, to ensure that MOUs always cover the data protection safeguards mentioned in these recommendations.
- As the information exchanges may be subject to multiple national laws and the supervision of multiple authorities, this single legal instrument should also provide clear provisions supporting **a closer cooperation** by the various authorities involved (DPAs, National financial regulators, FIUs etc).

4. Systematic **data collection** under CDD obligations should not be seen as a purpose in itself, but **applied to the risk** involved and take into account the data minimization obligation. The requirement to provide CDD related data should always depend on a pre-established risk assessment that takes into account different factors such as the situation of the client, the nature of the transactions, the financial product or the financial flows involved.

5. WP29 strongly supports the EU to press for **more consistency through EU harmonization** between the internal, external, global and specific regulations, approaches, practices and policies for AML/CFT processing operations[46]. In particular, major differences exist in the EU and national implementations and existing practices regarding elements such as the data retention periods[47] / mechanisms, the (availability of) accountability and reporting

---

[44] a.o. number 10 (page 6) of Opinion WP 168 on the Future of Privacy: Joint contribution by the Article 29 Working Party to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data, of 01 December 2009

[45] Number 13 (page 7) of Opinion WP 168.

[46] Corresponds with conclusion n° 4 of the briefing paper

[47] No data retention period or mechanism for FIUs, a data retention period of at least five years for institutions under the AML/CFT Directive, a data retention period of maximum 5 years in the negotiation directives for TFTP 2,... Current

schemes, the different implementation and interpretation of (indirect) access and rectification rights etc. This leads to legal uncertainty and ineffective AML/CFT processing operations and data protection.

6. WP29 recommends, in particular that any need for **new techniques of public or private sector exchange of information and cooperation mechanisms** should always be clearly **justified**. This justification should take into account the level of protection and effectiveness of existing AML-CFT cooperation mechanisms that already provide a certain level of data protection and/or judicial control with the same (foreign) counterparts. For instance, the added value of data protection under the TFTP2 Agreement[48] could be weighed against the value for effective data protection that is offered by some of the existing Egmont principles. The judicial approach via public EU judicial authorities has also clear data protection benefits. Existing forms of cooperation may help foster accountability[49], neutrality and therefore data quality[50].

Application of different forms of prior assessment[51s] of AML/CFT laws

7. ***Formal data protection assessment before the adoption of*** **AML/CFT laws.** One form of "prior assessment" of privacy and data protection compliance of a formal data protection assessment by a national regulatory authority before the adoption of national AML/CFT legislative instruments or measures based on such legislation (i.e. by financial regulators). There is a general impression that such assessments are very often not part of any formal adoption procedure of AML/CFT laws, or that the relevant authorities are involved too late in the process, when obligations are already adopted by the public sector[52.] With the exception of a few member states[53] where assessment is a mandatory requirement, financial regulators seem not inclined to proceed with a formal data protection assessment themselves or request an independent data protection assessment[54] before adoption of AML-CFT laws.

The general impression is that a great number of financial regulators and financial supervisors are not sufficiently aware of the implications that AML/CFT laws have on the right to the protection of personal data. As a consequence, an insufficient integration between such legislative measures has been identified in a significant number of cases, which makes it difficult to apply them consistently in practice.

---

practises of EU institutions are well beyond the term of 5 years and mainly depend on local interpretation. See also similar findings in the Report WP 29 01/2010 on the second joint enforcement action, compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive

48 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 the purposes of the Terrorist Finance Tracking Program, O.J. L., 195/5, 27 July 2010.

49 Via the judicial control on the sending and receiving of information and intelligence.

50 Work "à charge" and "à décharge", respect for the presumption of innocence and burden of proof, ...

51 Article 20.3 Directive 95/46/EC

52 See page 44, n° 105 of the LRDP report. This corresponds to a recommendation of the final report of LRDP Kantor Ltd and Centre for Public Reform.

53 i.e. a prior authorisation by the DPA exists in France. This DPAs services are also members of a special committee created by the "Commission bancaire" about the anti-laundering. This committee includes the FIU (TRACFIN), and representatives from the financial institutions and insurance companies. In Spain, for its part, it is mandatory that the DPA issues a report on the draft regulations implementing the national Data Protection Act (LOPD), which led financial regulators to consult the DPA before transposing the AML/CFT Directive into the Spanish law. The Spanish DPA is also full member of the Commission for the Prevention of Money Laundering and Monetary Offences, the board of directors of the Spanish FIU (SEPBLAC).

54 Article 20.1, 20.3 and 28.2 of the DP Directive

In an ever-evolving society with increased regulatory expectations[55] in both regulatory areas (AML/CFT and data protection), the national data protection framework and in accordance with the means and planning of national DPAs**,** prior assessment in preparation of new AML CFT laws should be considered **a mandatory requirement**[56] for financial regulators.

The **purpose** of such prior assessment should not be to provide a pro forma consultation for a formal privacy opinion ("a tick-box exercise"), but to provide effective data protection by implementing existing data protection rules and principles in AML/CFT laws in specific measures, and to increase the awareness and compliance with the current data protection obligations at all levels - financial regulators, financial supervisors, FIUs and institutions. The prior assessment process should, however, take into account any updates of AML/CFT laws and be undertaken before or shortly after the adoption of new AML/CFT laws, to guarantee that the respect for the data protection principles, rights and obligations are always guaranteed before and/or after the adoption of new AML/CFT measures.

8. **Data protection officials (DPOs).** The active involvement of an employee that has the required access and independence levels as (an additional)[57] data protection official[58] is another measure of prior assessment that has been introduced in some member states. To guarantee a balanced approach between AML/CFT and data protection, financial regulators should consider the introduction of such officials in countries where the existence of an anti-money laundering officer ("MLRO") is compulsory[59]. Furthermore, the functions of assessment of data protection compliance and compliance with AML-CFT laws should not be completely separated but integrated in a balanced way.

9. Within the last decade **other forms of prior assessment** have also started to appear. Presence of the DPAs in the FIU[60], or in other formal cooperation and/or reporting mechanisms in some member states are examples that could merit further discussion as an example for some other member states. Other forms of prior assessment which have been developed in recent years that can make the compliance with data protection requirements more effective include:

- privacy impact assessments[61] which are in line with the agreed method with the DPA (UK);
- a national privacy audit[62] for data processing operations (Netherlands) based on a previously established audit standard between the DPA and the auditing sector;
- an European privacy audit via the CEN[63] workshop agreements[64];

---

55 See page 7 footnote 31 of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

56 Pages 45, n° 108 and 51, n° 132 of the final report of LRDP Kantor Ltd and Centre for Public Reform mentions that Privacy impact assessments are becoming mandatory in many jurisdictions. This mandatory authorization by the DPA of AML/CFT processing operations is currently applied in France via a single sectoral authorization that is updated from time to time.

57 In addition to the normal data protection official for the normal processing of personal data of clients and employees.

58 See recital 49, 54 and articles 18.2 and 20.2 of the DP Directive.

59 For a list of such countries : see page 6 n° 10 of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

60 The FIUs of Spain and Norway are subject to specific forms of DP control (presence of DPA at the board as observer). However, other possibilities exist to respect also the requirement of effectiveness of FIUs.

61 See the ICO handbook on http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

62 Under the Dutch regime, an Dutch framework for a privacy audit was established a few years ago in cooperation with the auditing sector. See the Dutch link https://www.privacy-audit-proof.nl/

63 European Committee for Standardization

64 See http://www.cen.eu/cen/Sectors/Sectors/ISSS/CEN%20Workshop%20Agreements/Pages/DPPCWA.aspx.

- European privacy seal for specific AML/CFT tools - such a seal is currently offered by one DPA[65].
- self-assessment tools as developed by CEN[66]

The above examples may have a different scope, cost and value which should be carefully weighed and assessed by the data controller with the competent DPA and in accordance with the national data protection law. For instance: existing audits[67] may have only a financial or security scope, CEN audits tools may in themselves not necessarily incorporate and/or respect the position of DPAs and therefore lack official support..

10. The above forms of prior assessment should be incorporated into existing legislative procedures, structures[68], departments, audit committees or auditors established within financial regulators, financial supervisors, FIUs and institutions. Again, the aim should always be to offer real assurance via effective and adequate level of quality, independence[69] and guarantee for effective follow-up[70]. Furthermore, the choice about what form of prior assessment is preferred or required may be detailed by national DPAs in accordance with national laws. Finally, it might often be best "not to put all your eggs in one basket" (i.e. rely on only one form of assessment, such as a self-assessment tool or the in-house assessment that may lack the required quality and independence), but to combine different forms of prior assessment over time, taking into account a good balance between the cost and effectiveness, and including them in a coherent and systematic plan designed to promote compliance.

Transparency of AML/CFT laws and processing operations

11. WP29 refers to the requirement of transparency and foreseeability of the law under article 8 ECHR. More specific calls for transparency exist under the Recommendation CM/Rec(2010)13 of 17 November 2010 the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling[71]. WP29 is of the opinion that a **public and documented privacy / data protection compliance policy** should always be available. Again, this applies to different entities such as

- **Reporting entities** (i.e. credit and financial institutions plus natural persons, and in some jurisdictions, lawyers and notaries) should be required to provide their customers with a "**privacy notice**" making specific reference to the internal data protection policy in relation to AML/CFT obligations (in particular, the customer identification and verification process). These should apply and be clearly distinguished from policies that already exist for the purposes of the normal missions or commercial processing operations ("privacy" clauses in general terms and conditions of institutions and so on).

---

65 In Germany, European privacy seals are already provided for ICT tools by a department of one local DPA called "europrise". More info on https://www.european-privacy-seal.eu/

66 See ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16112.pdf

67 See the Directive 2006/43/EC of 17 may 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC

68 For instance a legal department, a compliance department, …

69 See the risk of conflict of interest in case such assessment would only occur by the in-house legal counsel, without adequate internal mandate and guaranteed follow-up for the EU part of the institution

70 Audit reports should be followed up and lead to effective, visible actions instead of running the risk to be locked up in the files of the audit department or the internal hierarchy.

71 Ref. CM/Rec(2010)13, published on https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029

- **FIUs and financial supervisors** should also publish, and keep up-to-date, **privacy policies**, setting out the categories of information it will require and hold under the AML/CFT legislation, for what purposes, and how they collect, use and disclose the personal data and information.

12. Public policies should be **readable and of good quality** and their role and existence should be well distinguished from the (extent of) the prohibition of tipping off. They should contain in a clear and accessible way (for instance via the technique of "short and layered" information notices explained below) and contain the following elements:

- the nature of the processing operations such as **identification** (KYC) and **profiling** (CDD) and the categories of personal data used (identifying data, profile data);
- the purposes of such processing operations. It is essential that a clear distinction between private risk management or general fraud management (sometimes via similar profiling techniques known as "credit scoring purposes") on the one hand and execution of AML/CFT obligations on the other is always made.
- citing the exact legal basis of the AML/CFT processing within the EU (i.e. clear verifiable references instead of general wording such as "the AML/CFT laws oblige us to");
- stating the qualification as data controller (of the authority, institution) for the respective processing operation and the identity of the representative and/or data processors (if partial or full outsourcing of AML/CFT processing is chosen[72]);
- citing the existence of appropriate safeguards such as:
  1. internal measures that the organization has established to tackle misuses, such as security breaches and the misuses of the reporting obligation[73] and feedback mechanisms;
  2. reference to any form of prior assessment that may be available (see above).
- Information that is necessary to guarantee the fairness of recourse to profiling such as:
  1. the categories of persons or bodies to whom or which the personal data may be communicated and the purposes of doing so (FIUs, intragroup communication,…);
  2. a clear procedure outlining how to exercise access (in some Member States indirect access) and rectification rights or file a complaint to competent authorities (DPAs, judiciary). This could also include a reference policy[74] (the exact procedure will depend on the member state and should be detailed as such);
  3. the persons or bodies from whom the personal data are, or will be, collected (i.e. PEP's);
  4. the compulsory nature of the reply to KYC or CDD questionnaires and the consequences of not replying for the clients;
  5. the applicable data retention period and/or data retention mechanism;
  6. the envisaged effects of attributing a profile to the client; and

---

72 The global services industry is already evolving towards outsourcing the "know-your-customer" process in banks and to pool information from different banks (not just from the group) in a single database

73 One FIU argued that for certain STRs it is sometimes wondered what the source of information is. It has already been observed that an increase in STRs comes immediately after that the arrest of a certain client was reported in the newspapers, which shows there is a real risk of confusion between risk management of reputation and a risk based approach in relation to the fight against money laundering.

74 Institutions, FIUs and bank supervisors should also be recommended to refer any complaint (that they are aware of) on principles set out in the DP Directive to authorities that are competent under article 28 of the DP Directive (DPAs or judicial authorities). In case of doubt, they should contact the DPAs for an opinion on compliance with DP provisions

- As well as any other information as appropriate (such as recommendations set out by the Council of Europe for profiling[75]).

13. Whilst many direct measures are clearly visible to data subjects, if such measures cannot be clearly or solely justified based on commercial purposes[76], this raises concerns. Such measures include specific AML-CFT questionnaires that aim at to fulfil KYC and CDD obligations, or (in extreme cases) the blocking of accounts or the refusal of services. For such measures, the technique of **"short and layered" information notices"** should be applied. These should include elements such as the following:

- when clients receive a questionnaire, they should receive (or be able to refer to) **additional and clear information** from the institution, containing (at least) a clear and correct description of the purposes and laws on which the additional information is requested[77].

- when blocking accounts or refusing services based on AML-CFT grounds, the use of the prohibition of tipping off exemption should only be used following the specific analysis or follow-up. Furthermore, institutions should at least be able **to refer** to their public compliance policy, access/mediation process handling procedure before any referral to effective redress via the DPA or the competent jurisdiction (DPAs or courts).

14. Considering the fact that AML/CFT laws are likely to present specific risks to the rights and freedoms of data subjects, WP29 considers it an essential requirement that each public authority or private organization that is a data controller or data processor of AML/CFT processing operations provide **internal, confidential data protection policies** pursuant to the application and follow-up of the prior assessment method. The relevant policies, documents, audit reports and management decisions should be readily available, as they may be requested by DPAs in accordance with their national policies and procedures.

In order to be effective, the internal data protection policy should be as objective as possible and cover the following areas as understood by the WP29, the EDPS or the competent DPA:

- internal staff training on privacy and data protection issues in addition to AML and CFT issues (e.g. internal DP and AML listing and delisting procedures, internal and external motivation of reporting decisions, decisions based on CDD processing).
- identification of good and bad AML/CFT practices in the light of European human rights requirements by relevant authorities (financial regulators, financial supervisors, FIUs and DPAs) and institutions, in particular for the execution of obligations such as KYC, CDD, reporting and feedback. I.E. what practices are considered below data quality and data protection standards? Examples of bad practices include the processing operations which are disproportionate in the fight against "serious

---

[75] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies, published on http://www.coe.int/defaultEN.asp

[76] Including blacklisting of clients, blocking of accounts, refusal of services, unilateral termination of the services agreement based on the execution of CDD obligations

[77] One example of vague or unclear reference is that of a French institution that requested additional client information due to the "regulation on the knowledge of clients"

crime"[78], such as when processing serves more general purposes such as "fraud management" assessments. Other forms of disproprtionate assessment are the ones that are solely or mainly based on newspaper articles, statistics or typologies related to ethnic background.

- listing and delisting procedures in accordance with European human rights such as the right of defence - in particular the right to be heard, and the right to effective judicial review of those rights before independent DPAs or local courts.
- procedures that prevent and remedy the risk of identity theft. In particular, different and subsequent procedural steps should be taken by institutions and FIUs to prevent, detect and remedy different forms of illegal use, copying or theft of identity documents and data, as well as information that may lead to "identity theft".
- the principle of "ensuring accuracy" of public sources (newspapers, search engines)
- the obligation to store the exact data source and date for each information or assessment, in order to verify the age and accuracy of the application under the DP obligations
- the screening of the relevance and necessity of questions in client questionnaires
- a clear description of, if and how, the organisation makes a distinction between factual data, intelligence data (profiling, STR's etc), and the data collected for different categories of data subjects[79] (clients, employees) along with the different purposes of processing in the institution (client management, HR management, compliance).
- a description of the risk assessment criteria and procedures
- a description of the decision-making procedure, especially for assessments with a tangible impact on an individual data subject, such as blacklisting of clients, the blocking of accounts, refusal of services, unilateral termination of the services agreement. The internal decision process and motivation should be clear, adequate and precise in the light of the relevant purpose.
- a procedure for the right to object on the grounds set out under article 14 (a) of the DP Directive. An example might be cases relating to visible AML/CFT measures that are similar to the cases that were successfully challenged before courts of any member state, the ECHR or the Court of Justice.
- mechanisms for re-assessment and periodic review.
- communication to respective AML/CFT authorities of at least the "management summary" of any such assessment and procedure for such authorities to obtain a copy of the full assessment, upon request.

Obligation of purpose limitation – Onward transfers (in and outside EU)

15. Due to the continued global reinforcement and extension of the institutional secrecy working against "dirty money" and its application to an increasing number of serious criminal acts and risks (the financing of terrorism, transnational organized crime, illicit drugs and the financing of the proliferation weapons of mass destruction[80]) shows that, over time, an increased number of criminal acts and risks are considered to be either connected to terrorism in any of its forms, and therefore going beyond the original purposes of anti money

[78] As mentioned in recital 7 of Directive 2005/60/EC (initially limited to drugs offenses). See also the risk of function creep linked to wide interpretation of (general) "fraud management".

[79] Point (d), page 11 of the Ludford Report.

[80] See UN Security Council Resolution 1373 that refers to a close connection between these acts and the focus of the FATF recommendations that shifted after 9/11.

laundering. Thus the application of exceptional AML/CFT obligations by the private sector is warranted.

In this area, a clear risk of function creep exists. Once the level of "serious criminal acts and risks" is in practice surpassed and extended to, i.e. the processing operations for (general) "fraud management" and the management of reputational risks of reporting institutions, the obligation of purpose limitation is clearly no longer respected.
There are practical consequences by not adhering to the purpose limitation principle. For example:

- Increased risk management for an increased number of different acts and phenomena leads to an increased cost, back-log, lack of internal expertise and ineffective and a disproportionate fight against money laundering and terrorism financing by institutions. This cannot be sustained in the longer term by the private sector that serves a different core business and interest.
- the approach of over-securitization and over-classification for an increased number of acts also leads to ineffective use of public resources. See in this respect the recent (de)classification guidance review of the US administration[81].

Therefore, AML/CFT laws, compliance policies and cooperation mechanisms should return to apply a **strict and clear application of the purpose limitation principle** for the primary and onward transfers[82], clearly excluding the use for other purposes such as general "law enforcement", "policing purposes", the enforcement of tax laws which are justified under other conditions for processing.

16. The purpose limitation principle should be rephrased for AML/CFT purposes at the FIU level. Even if this principle is badly or (at least not clearly) implemented under the Framework Decision 2008/977/JHA, it is still a clear principle that has to be respected under existing privacy and DP regulations such as Convention 108 and article 8 ECHR.

Quality and awareness of AML/CFT laws

17. In order to enhance the quality of AML/CFT laws and awareness of DP obligations and principles, WP29 recommends that discussions amongst DPAs, FIUs and financial regulators should continue through different platforms, including the WP 29 (financial matters subgroup) and the FIU platform. One of the possible ideas that could be developed further is the discussion on conditions*83* for the use of the FIU consent and/or MOUs as a guarantee of adequate data protection.

---

81 See in this respect the Fundamental Classification Guidance Review of the Obama Administration by the Executive Order 13526 of December 29, 2009, published on http://www.fas.org/irp/offdocs/eo/eo-13526.htm . The purpose of the Review is to evaluate current classification policies based on "the broadest possible range of perspectives" and to eliminate obsolete or unnecessary classification requirements.

82 See the criticism on the TFTP2 Agreement that provides only guarantees for the first level of transfer (EU-UST)

83 One condition might relate to the status and capacity of the FIU to assess data protection requirements in a adequate and independent way. Sometimes FIUs are a police service, sometimes FIUs are independent administrative or judicial bodies. The risk exists that FIUs consider their AML/CFT tasks as core business, and human rights requirements as a burden for the effective fight against terrorism or money laundering. Instead, a balanced approach should be the ultimate goal. Here it might be worth to investigate whether the threat of refusal of consent could be considered a "negative" procedural DP safeguard to establish ownership, accuracy of intelligence and blocking of data transfers that clearly violate the purpose limitation principle, and the adequate data protection principle (in case the FIU is not present in a country with adequate level of DP protection pursuant to decision DPA or EC).

Data quality – measures to ensure data accuracy

18. Reporting entities and FIUs should take all reasonable measures to ensure the accuracy of personal data before they collect, use or disclose such data.

In particular, reporting entities should

- confirm the accuracy of information before transmitting a suspicious transaction report (STR) to the FIU.
- take all reasonable measures to ensure that the information they acquired under the KYC and CDD obligations remains correct and protected from misuse or loss and from unauthorized access, modification or disclosure throughout the data storage period. For this purpose, **periodic review of the quality of the data**[84] and of the data profiling / data mining techniques should be implemented within a reasonable timescale[85]. Review criteria and control should not be left to internal and arbitrary discretion of institutions (HQ or branches), FIUs, police services or subcontactors (e.g. commercial sale of AML/CFT data such as PEP lists etc). Any review should also cover the deletion of inaccurate or old data that has passed the maximum data retention period, and should not just cover renewal mechanisms.
- as a means of ensuring proportionality and data quality, use **harmonized STRs** through the production of standardized forms, including mandatory fields that are to be completed.

19. Any **typologies**[86] published by FIUs should be accompanied by a clear FIU **disclaimer** that refers to the purpose and risks of possible misuse of such typologies by institutions.

20. It should be taken into account that profiling is a complex matter. The WP29 is of the opinion that profiling obligations for AML and CFT purposes and related operations[87] are lawful in so far as they concern legal obligations that are provided for[88] by EU and domestic AML and CFT laws. However, these obligations cannot be met relying solely on free and specific consent of the data subject (see above) and **profiling has also serious side-effects and inherent limitations**. These side-effects and limitations are:

- the "base-rate fallacy" (lack of accuracy) shown by the number of false positives[89] or false negatives[90]. Profiling using false positives means that attributes are (or could be interpreted to be) highly likely to result in non-money launderers and non-terrorists being prevented from accessing financial services, whilst "negative positives" mean

84 See the periodic review obligation in articles 5 and 9 of the framework decision 2008/977/JHA.
85 See point 3.10 of the recommendation CM/Rec(2010)13
86 In the AML/CFT context, the term "typologies" refers to the various techniques used to launder money or finance terrorism (definition given on http://www.imf.org/external/np/leg/amlcft/eng/aml1.htm)
87 data warehousing and data mining, risk assessment, the use of typologies and other operations under CDD obligations, blacklisting, …
88 See n° 117 of the explanatory memorandum of the recommendation CM/Rec(2010)13, published on https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029 "Money laundering regulations" are a specific example.
89 identifying innocent people as suspects
90 not identifying real money launderers or terrorists

there is no absolute guarantee that all money launderers and terrorists will be intercepted, a.o. due to the adaptive behavior of real suspects[91];

- Whilst there is no question about the importance in tackling the financing of terrorism, such an approach as described above, inevitably infringes upon other fundamental rights. Any approach adopted should always bear in mind the balance required to the issues of terrorism with that of the legal and human rights of the data subject.
- there is also evidence to suggest, that the targeting of a 'suspect community' can be wholly counter-productive by undermining counter-terrorism efforts and fuelling radicalization; and
- the clear lack of consensus in both EU[92] and US studies on (the conditions for) an effective risk based approach (profiling for counter-terrorism purposes) is, therefore, not a coincidence.

Therefore, while not calling into question the legitimate aim, the pressing social need of specific profiling obligations and being in line with the recommendations of the Council of Europe on profiling[93], the above factors do illustrate the need to adopt **appropriate safeguards in domestic AML and CFT laws for every profiling operation, and is even more important in cases where sensitive data is involved**[94]. As stated before, profiling operations in the context of AML/CFT cannot be based on the (free) consent of the client[95]

Such appropriate safeguards could consist of statutory regulation of the intended profiling process, a.o., via guidance, examples and strict conditions to ensure that profiling practices remain within the boundaries of correct, legally transparent[96] profiling. Conditions, risks and guarantees should first be documented and made available by financial regulators and financial supervisors instead of submitting the total population to the risk of ineffective and incorrect application or interpretation of profiling obligations[97] by institutions.

Clear examples of ineffective and unlawful execution of risk based obligations that were given are, for example, based on a single non-verifiable criterion, such as newspaper articles, public search engines or risk assessment based solely on the occurrence of sensitive characteristics relating to ethnicity (religion, national origin, language or tribal affiliation and so on) or implemented without appropriate safeguards (see infra).

21. Any **feedback** should be accompanied by **a clear FIU disclaimer** that refers to the purpose and risks of possible misuse of such feedback by institutions.

---

91 See page 14 of the final report and the last paragraph of page 7 of the Working paper N° 1 of the Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, published on http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

92 See page 7 of the study ordered by the European Commission by Brown, Ian, Working Paper N° 1, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments , published on http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

93 Principle 3.11 of the recommendation CM/Rec(2010)13

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

95 See above regarding the lack of consent of clients in the context of AML-CFT processing. See also point 3.5. of the recommendation CM/Rec(2010)13

96 In the meaning of foreseeability of the law (article 8 ECHR).

97 See the conclusion of the report mentioned in the previous note.

22. A "**balanced" use of feedback** mechanisms should be recommended. I.E. any **feedback mechanism** should include safeguards to protect the rights of data subjects. Feedback mechanisms should in particular:

- be applied by FIUs on a case by case basis instead of as a general rule or obligation;
- concern only final decisions of national administrative or judicial authorities, I.E. excluding preliminary judgments;
- be undertaken by FIUs in a context of full cooperation with the local judicial authorities, for example by informing the institution of a final judicial decision, or a decision not to prosecute ("sepot");
- be sufficiently detailed to be useful to the reporting entities yet suitably limited to avoid prejudicing professional secrecy, personal privacy or investigative proceedings. This is of particular importance if information from the reporting entity has been forwarded to the judicial authorities about any individual which could prejudice either their privacy, or their entitlement to exercise their legal rights. Therefore any use of either general feedback or specific (individual) feedback should be based on objective data (facts) instead merely of subjective appreciations of facts (suspicions, risk factors etc.). However, FIUs should still be able to follow up on STRs by asking more relevant questions during investigations.

Proportionality and data minimization principles , data collection and data sharing

23. WP29 questions the necessity of projects or transpositions of national financial regulators that go further than the requirements or literal transposition of EU AML/CFT regulations (aka process of **"goldplating**" of AML/CFT obligations), when those transpositions affect even further the right to data protection, and especially when they occur without any formal data protection assessment.

24. The AML/CFT legislation (in particular, Directive 2005/60/EC) does not sufficiently specify the kind of data[98] that are collected and exchanged. The abovementioned provisions give very broad definitions and outlines the risk of disproportionate exchange of information. Consequently, WP29 recommends amending the Directive and/or guidance by financial regulators **to specify the kind of data**[99] to be collected and exchanged and inserting the word "legally" "obtained" under art. 21(3).

25. The institutions questioned whether **intra-group sharing** of information meets the data protection principles of necessity, proportionality and purpose limitation[100]. There is a clear debate under the different AML/CFT laws on the permitted vs. required **form of data sharing** (and risk analysis) of customer information. This is further complicated by the possibility of either centralisation or decentralization of the compliance function in institutions. For some, it would appear to some that only the most invasive and far reaching forms of data sharing such as via data consolidation at international group level[101] with state of the art data mining functionality and/or via full outsourcing of the AML/CFT service to

---

98 Art. 8 of this Directive, in the context of the customer due diligence by the reporting entity, refers to "documents, data or information obtained from a reliable and independent source", whereas art. 21(3) lays down that "FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfill its tasks."

99 See infra the main difference between the categories "identifying data" and "profiling data" discussed under the topic of data retention

100 See annex 7 (page 59) of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

101 Such as of the national backlists.

specialized third parties would be adequate for AML/CFT purposes. For others, customer and transaction monitoring at group level is not practical because a case-by-case justification is required[102] and data centralization creates additional national data protection compliance[103] and data quality and analysis risks. It should be recalled that the WP29 and EDPS[104] have recommended in the PNR[105] and (more recently) the TFTP cases[106] that systematic use of a (proportionate[107]) **"push" instead of a "pull" system** should be applied when meeting the proportionality requirement. This principle was applied in the relationship vis-à-vis US and EU authorities, and air carriers and should also be applied by multinational institutions.

26. There appears to be a conflict between the repeated calls and obligations in 15 EU member states[108] for consolidated (global) data management and risk management in the area of AML/CFT on the one hand, and on the other, the obligation to guarantee a level of adequate data protection as understood under the general privacy and data protection framework of the EU and the Council of Europe. Even though some operations at FIU level, such as the existing STR and feedback mechanism still appear to be working as a "push system", there has been a clear encouragement by the EU financial supervisors[109] and the Basel Committee over the years for risk management and assessment to be undertaken at group level (**global risk management**) and its primary focus has been around efficiency, cost and uniformity of the AML/CFT processing operations. The model of global risk management was also introduced without any proper and independent privacy impact assessment. Based on the requirement of combined application of the AML/CFT and the DP framework, **a more balanced data sharing (push) scheme should be the norm that also provides adequate data protection**. For instance, this balanced data sharing scheme could incorporate **segmented risk management at local level in jurisdictions with adequate data protection**)[110], local assessment and local management, taking into account the prior assessment competences of national DPAs and the different national data protection compliance requirements for a.o. the protection of sensitive data, blacklisting and so on. This also applies to any form of AML/CFT services that may vary from the sale or distribution of AML/CFT information such as via blacklists, PNR lists etc. to more advanced outsourcing services.

---

102 See annex 7 (page 59) of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

103 See the reference to sensitive data such as reference to ethnic origin or religion.

104 See § 98 of the Opinion of 20 December 2007 on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes "The EDPS recalls that the push method, allowing airlines to keep control on the quality of data transferred and the circumstances of transfers, is the only admissible method with regard to the proportionality of the processing. Besides, it must consist of an effective push, that is, the data should not be sent in bulk to an intermediary but filtered at the very first step of the processing. It is not admissible that non necessary data — and data not included in Annex 1 of the proposal — be sent to a third party, even if those data are to be deleted immediately by this third party."

105 See Opinion 122 of the WP 29 in the PNR case

106 The (non published) EDPS comments of 3 July 2009 to the negotiation directives for an EC-US (UST) "TFTP agreement" contain a recommendation to transfer data through a "push" rather than a "pull" system, with a record of every transfer of data that is taking place. This records should be made available to competent DPAs upon request.

107 Not a "bulk push" of data. See n° 84 and 98 of the opinion of the EDPS on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, OJ, 1 mei 2008, C110/1. : "not be sent in bulk to an intermediary but filtered at the very first step of the processing"

108 See page 5 paragraph 7. of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

109 See pages 4 n° 4, 5 n° 7, 6 n° 9, of the EC, DG MARKT, working paper SEC (2009) 939 final of 30 June 2009

110 Such as in the case of SWIFT

Data retention

27. At the moment, Directive 2005/60 establishes a minimum[111], but **not a maximum data retention period**. Also, it only applies to (as stated under article 30) to reporting entities[112]. The WP 29 took also note of the position in the EC Regulation N° 1781/2006[113] on data retention. The WP29 is as well of the opinion that the current wording of the AML/CFT data retention schemes is unclear. Considering both factors (i.e. lack of clarity or no specific maximum retention periods), **the WP 29 is of the opinion that the current AML/CFT data retention schemes give room for interpretations that could create an unacceptable risk of 'evergreen' data retention** when the current AML-CFT rules are applied in practice by institutions. Evergreen storage of data cannot be deemed compatible with the data protection requirements of proportionality and data minimization. Data retention schemes can**not** imply **an evergreen right** for institutions, law enforcement agencies (FIUs or other authorities) when processing either identifying data (KYC) or risk assessments (CDD and STR related data) particularly if processing in question has been based on the unilateral assessment of the institution, FIU or other authority to store data for potential undefined future uses or other assessments.

Instead, **data retention laws and provisions should be clear and well documented** in all relevant EU and national AML/CFT laws, and apply to all relevant parties that are involved in the processing of data for AML/CFT purposes (including but not limited to institutions, FIUs and financial supervisors). The aforementioned need for consistency through harmonization **for (i) reporting entities and (ii) FIUs** would ensure a level playing field between economic operators (reporting entities), and increase the efficiency of the information exchange between FIUs.

28. Data retention schemes in the context of AML/CFT processing **are a complex issue that deserves a more balanced approach than can be achieved with the application of simple data retention periods that would seem to cover all situations for an undetermined maximum data retention period.** As explained below, the WP 29 identified different factors that impact the necessity for further data retention and that should be taken into account in AML/CFT laws and polices. Those elements are :

- the nature of the data (data categories) and form of data storage (coded and non-encoded access for operational AML-CFT purposes)
- the need for continued data accuracy assessment, and the possible impact of such assessments. Further storage of obsolete or incorrect data under data retention periods without periodic assessment of the data accuracy and data minimization principles (i.e. a model of "AML/CFT fridge[114]" at compliance departments or FIUs cannot be justified. I.E. Any data controller has the obligation to periodically assess the data

111 at least five years after the end of the business relationship with the customer or after the carrying out of the transaction

112 Against such background, the WP29 recalls the Opinion of EDPS on the proposal for a Council Regulation on administrative cooperation on combating fraud in the field of value added tax (recast), published on the Official Journal of the European Union of 17.3.2010, C 66/1, paragraph 46: "There is no justification given for such a storage period. If personal data are involved, providing for a minimum period without any reference to the necessity principle is contrary to the requirement of data protection legislation that data should not be stored longer than necessary. The EDPS therefore encourages to reassess this provision (…) and determine a maximum storage period in case personal data are concerned, with possible exceptions only in exceptional circumstances."

113 Regulation of 15 November 2006 on information on the payer accompanying transfers of funds, OJ L345/1, 8 December 2006.

114 See the analogy with the "FTC spam fridge" of 1998. Since 1998, the US Federal trade Commission has asked people to forward any and all spam to a special e-mail address.

accuracy and the further need to store older risk assessments and the need to continue to process older CDD data.

- the different processing operations and legal basis of data controllers (Institutions, FIUs,…)
- the need for accountability and independent oversight on a correct application of data retention schemes by institutions, FIUs and judicial authorities (this need goes beyond the necessity of data retention for operational purposes).

29. Data retention schemes and data retention periods should make a distinction between extracted/used and non extracted / non used data. Also, differences in data categories exist such as between identifying data (KYC data: name, address etc) and the more subjective or sensitive information linked to "profiling data" (CDD data: profiles, secondary information derived from analysis and external sources, and so on).

The AML/CFT data retention mechanism in article 30 of the AML/CFT Directive is complex, as it contains two elements: reference is made to a fixed data retention period of 5 years, but article contains also an extension mechanism. Also, confusion is made in the mechanism as it does not distinguish clearly the continued obligation to store data on the one hand of reporting entities (obligation lasts at least as long as the client relationship exists) from the need to store a specific type of data set. For the second element, the impact of intervening factors on the real need to store data is not taken into account (data accuracy is not static during the client relationship, nor is evergreen retention as such justified)

WP29 recommended previously that, as a general rule that, **a general data retention period must be clearly regulated and as short as possible**[115]**, without evergreen extension mechanism (see before).**

This means that the fixed retention period of 5 years should start at the date on which the data was first obtained, rather than on the date of the end of the business relationship or the carrying out of the transaction;

Also, to avoid evergreen data retention, the extension possibility beyond the initial fixed retention period of 5 years offered by article 30 (a) and (b) of the AML/CFT Directive should be as short as possible. This means that

- access for operational AML/CFT purposes **of subjective personal data** (risk analysis, client label or category, applied typology or profile, CDD data,…) **cannot exceed five years from the date at which such assessment was made for AML/CFT purposes. Again, continuous data accuracy assessment of risk assessments should be made, and "AML/CFT fridges" of old profiles and assessments beyond 5 years seems unnecessary.**

- access for operational AML/CFT purposes **of objective personal data** (transaction data, KYC data), means that such data **should only be kept longer than 5 years, provided that the data accuracy of such is data is continuously reassessed and confirmed (see above under data accuracy).** For instance, such reassessments

[115] See page 6 of Opinion WP 113 of 21 October 2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC

should deal with the lack of need for further storage of old standard ID documents that are renewed over time).

30. WP29 recommends that for each piece of information or for each assessment a **source and date should be encoded**, to enable the calculation and justification of the correct data retention period for each piece of information (or analysis) from the data such information was first obtained or from the data of such risk assessment (STR,…), either directly from the client or indirectly (feedback, cooperation within a group). Information for which the exact source or date cannot (or can no longer) be traced should be immediately deleted, either by the data controller or on request of the supervising authority.

31. In principle, all information about the transaction, the STR and risk assessment itself, should[116] be **deleted (or unencoded access for operational AML-CFT purposes by the compliance department blocked**[117]**) immediately and automatically** when a specific **suspicion is rebutted or an AML-CFT investigation** or suspicion that is based on such specific elements has **ended**. Blocking, erasure or destruction of personal data must also be carried out by the institution or authority in case **order,** and block, erase or destroy such personal data when a competent DPA or a (final) decision of a court or judge-magistrate[118] that is competent to intervene for important acts in an ongoing criminal investigation[119]. Any in-house assessment of the necessity for ongoing investigations should be readily available (encoded or justified) via periodic (re)assessment in case of intervention of a competent supervising authority (financial supervisor, DPA or court). The practice of "**flagging**" data[120] instead of the deletion of data or the blocking of unencoded access for operational AML-CFT purposes does not constitute an adequate or equal guarantee compared to measures of deletion or blocking access for operational purposes, as such further unencoded data retention may encourage cause further use and even 'evergreen' data retention.

32. **Beyond the maximum period of five years** mentioned in recommendation 29, **a mechanism for limited renewal** of such a period should only be available[121] for the data

---

116 Taking into account the obligation to delete or rectify incorrect data, and combining it with the obligation to limit the storage of data no longer than is necessary for the intended purpose

117 Longer data retention periods may be applicable and required for different needs than require for the operational AML-CFT processing operations of compliance departments such as keeping evidence of fulfilling AML-CFT obligations vis-à-vis the financial regulator and/or central compliance department. This does not warrant further unencoded access for operational services however.

118 For instance onderzoeksrechter (Belgium), rechter-commissaris (Netherlands)

119 Article 28.3 Directive 95/46/EC.

120 blocking is usually identified with labeling (≈ flagging) personal data in such a way that their further processing is restricted (i.e. Slovenian Data Protection Act).

121 This is a slightly stricter version of the Norwegian data retention scheme. The FATF evaluation of Norway (page 50, n°. 153). describes the Norwegian data retention process as follows : "If a suspicion of ML/FT is rebutted, all information about the transaction and the STR itself must be deleted immediately (Norwegian MLA law s.10). If the suspicion can be neither rebutted nor confirmed, the STR is filed for intelligence. After five years, all information about the transaction must be deleted if no further information of importance is registered, and no investigation or legal measures initiated against the legal or natural person. On the other hand, if new information of importance is registered, a new five-year deadline shall apply from the date of registration (Norwegian MLA law s.10). The MLU places a strong emphasis on the protection of privacy. The information contained in its database can only be accessed by the MLU staff, the Proceeds of Crime team at ØKOKRIM and authorised persons (such as the head of ØKOKRIM). The MLU's work is largely governed by internal guidelines that are intended to ensure prudent and secure handling of STRs. For instance, the MLU must destroy/delete all the information that has been registered (including the STR itself) if the suspicion is rebutted at the stage of the initial examination of an STR (Norwegian MLA law s.10)." See also the articles 4, 5 and 9 of Council Framework Decision 2008/977/JHA describe a mechanism that enables calculation of the correct maximum retention period ("time limits for retention of data"), with respect for ongoing investigations or prosecutions. This applies "in criminal matters".

stored by authorities such as FIUs. Such a mechanism should only be invoked in cases where either, as in some member states (i.e. Italy) a court or judge/magistrate or b) an appropriately designated senior official within the FIU (i.e UK) has undertaken a risk assessment based on all applicable laws and have good reason to retain the data beyond the five year rule. Furthermore, any law affecting this procedure should contain the provision to calculate the end term for the retention mechanism (see above).

Qualification as data controller

33. Under their current AML/CFT obligations **FIUs and institutions** have a high degree of decision-making power to define the purposes and means of their processing operations such as via the KYC obligations, the handling of STRs or the sending of feedback. Applying its previous opinion WP 169[122], WP29 is of the opinion that the above situation indicates **a role as data controller** instead of data processor. This qualification triggers the responsibility for data protection obligations under the data protection regulation.

Independent data protection control of AML/CFT processing operations

34. In countries where there is an indirect right of access[123], the (conditions for the) indirect access rights via DPAs should be deemed applicable and developed further by national legislators to ensure that these access rights are not excluded in relation to AML/CFT processing operations by FIUs, financial supervisors and institutions. In countries where the law foresees no indirect access right[124], the supervisory powers of DPAs to supervise and handle complaints[125] should be applied. In any case, DPA's remain free tot determine the conditions for the admissibility and policy for the handling of complaints, in accordance with their national law. Also, WP29 recommends further investigation to develop a **more uniform approach at EU level**, via EU regulation or the adoption of models or guidelines for **both forms of supervision via DPAs** on personal data processed by reporting entities and FIUs. These guidelines should allow the competent DPA to gain access to and review data held about a data subject, and after consultation of the reporting entity, FIU or financial supervisor determine whether (any or limited) access can be provided to the data subject without prejudicing law enforcement operations or investigations and the prohibition of tipping off, if the data subject has already been refused access by the reporting entity or FIU or such direct access is not available to the data subject.

35. In order to fulfill the required roles of guidance (awareness raising and training, …) and supervision of DPAs mentioned under these recommendations, additional **financial and human resources** should be made available.

Fair processing

36. The practical meaning of the principle of **"fair and legitimate" processing** should be developed and applied to AML/CFT obligations or techniques[126] that contain specific data protection risks such as the KYC (profiling) and CDD obligations and the reporting and feedback obligations. This means that both legal and illegal interpretations of such

122 Opinion WP 169 on the concepts of "controller" and "processor" of 16 February 2010.
123 Belgium
124 Greece, Netherlands, Spain, …
125 Article 28 Directive 95/46/EC
126 Point 16 of the draft recommendation on profiling.

obligations should be discussed between authorities, DPAs and institutions. Also, any practices, such as KYC / profiling, CDD, and the application of reporting and feedback obligations etc should be applied in line with applicable EU or national law and internal and external data protection compliance policies and European human rights requirements.

Protection of sensitive data

37. In the line with previous recommendations of the Council of Europe[127], WP29 is of the opinion that collection and **processing of sensitive data** for the purposes of AML (linked to serious crime) and CFT is prohibited unless the necessity of such profiling can be proven by the institution and as long as legislators and financial regulators have also specified "**suitable safeguards"** in AML and CFT laws. Such safeguards should aim to avoid and sanction "goldplating" and arbitrary interpretation of (especially) profiling obligations **under CDD obligations** by financial regulators and/or institutions. Simple reference to a legal exemption or a legal obligation to profile is clearly inadequate as it does not add any specific safeguards to process sensitive data. Specific measures that aim to implement these recommendations, however, may constitute suitable safeguards in accordance with the applicable national data protection law.

Security of processing operations

38. WP29 recommends financial regulators and institutions to **take measures to prevent and remedy cases of identity theft that are also aimed** at dealing with the privacy (identity) issues of the possible victims of identity theft.

Adequate data protection –Proper legal basis for transfers (primary and onward) transfers / international exchange of personal data

39. Some institutions and FATF seem to assume that instruments that are mainly developed for international transfers for commercial or human resources management purposes (safe harbour, contractual clauses, BCRs,…) would be also adequate to "address the obstacles to cross-border exchange", and that the public interest grounds of foreign authorities in areas without adequate data protection would be, as such, a valid basis for the processing of personal data. Such authorities (including FIUs) are, however, established within areas without adequate data protection and are not bound by the group/institutions privacy policy or other solutions that were developed by the EU for the normal transfer of commercial data (example : contractual clauses, BCRs,…). As shown in the PNR and TFTP cases[128], **political solutions** should therefore also be developed at EU level via international agreement, in order to provide binding obligations for the authorities that receive AML/CFT personal data and are established in countries without an adequate level of data protection.

40. **Adequacy** findings cannot be left to the arbitrary discretion of data controllers and should **always contain a rigorous process** that contains a comparison of the level of protection provided **in the specific country** with EU privacy and data protection standards [129]

---

127 Council of Europe, point 3.11 of the recommendation CM/Rec(2010)13

128 See however the reservations of the WP29 on the TFTP Agreement, published on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_06_25_letter_to_libe_en.pdf

129 Such is both the case under UK law as under the TFTP2 agreement where the UST is "deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the

by DPAs and/or the European Commission as described under articles 25.2, 25.3 and 25.6 of Directive 95/46/EC. Other methods that are sometimes called upon such as the findings relevant to commitments of data controllers or data processors, commitments in single instruments such as international agreements, MOUs or legal opinions by third parties may not in themselves be sufficient or impartial enough to constitute a valid adequacy finding.

With respect to **onward transfers of data from EU FIUs**, a distinction should be made between (1) the exchange of data between FIUs established in Member States[130], and (2) the exchange of data from FIUs located in the EU to those in a third country (i.e. FIUs participating in the informal worldwide network referred to as "the Egmont Group"), via the secured network "Egmont Secure Web").

41. For the exchange of data between FIUs of EU Member States, WP29 finds that **the Council Decision of 17 October 2000[131]** should be replaced with a new Council decision (see above). Points of particular concern in the light of (mainly) the principles of proportionality and purpose limitation are :

- a stricter definition of the categories of data to be exchanged and of the purpose[132];
- specification of the "competent authorities" to which, under article 2 of the Council Decision, data and information may be made available;.
- to add an explicit reference in article 4.3. to compliance with data protection principles and legislation as a reason for FIU to refuse to divulge information to another FIU;
- specifying in article 5.1 "information and documents (…)" (that) can be transmitted and "are intended to be used for the purposes laid down in article 1(1)."

42. In addition, WP29 welcomes the adoption by FIUs of **standard request forms** to standardize FIU-to-FIU exchange of information requests. In fact, pre-defined requests, including pre-defined questions and other data fields (adequate, relevant and not excessive), can enhance transparency and proportionality of data transfers.

43. **The value of MOU's between FIUs as data protection safeguard** is often questioned. Even though MOUs may not always ensure an adequate level of data protection within the meaning of article 25 (2° of Directive 95/46/EC (see above in rec 40), the WP29 recommends the following:

European Union to the United States for the purposes of this Agreement" (n° 75 and 76, page 36 of the final report of LRDP Kantor Ltd and Centre for Public Reform)

130 pursuant to art. 38 of Directive 2005/60, regulated under Council Decision of 17 October 2000, via the network "FIU.Net";

131 Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000, p. 4–6

132 article 1.2 refers to the exchange of "any available information that may be relevant to the processing or analysis of information or to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved". Such notion of "any information" is too broad and entails the risk of disproportionate information exchange. Besides, the purposes for which information may be made available are also very general, which runs counter to the general data protection requirement that the purpose must be specified and made explicit. The respect of such requirement is accrued by the circumstance that the FIUs, having different roles and functions, differ in relation to the powers conferred on them by national legislations, varying from administrative to police cooperation, and, possibly, even secret service.

- the issues relating to data protection should be adequately covered by the MOU. These issues include, inter alia, an escape or termination clause considering the possibility for DPAs and the European Commission to monitor the adequacy of the data protection in relation to the transfer and processing of data from one country to another and the necessity and proportionality of such transfer. The MOU should specify the kind of personal information that can be exchanged, circumscribe the purposes for which personal data can be exchanged and assure that the necessity principle is respected;
- the European Commission, after consultation with WP29 and the FIU platform, should consider developing a standard MoU incorporating such privacy concerns;
- the standard MoU should also be the object of periodic reviews by DPAs; and
- since the FIU should be considered a data controller[133], the refusal of its consent for first transfer or further use of AML/CFT data could work as a negative data protection safeguard. I.E. even though the consent in itself cannot establish the adequacy of the data protection regime for the receiving country, the FIU should withhold its consent in case of clear violation of DP rules or for requests for transfers to countries without adequate data protection. The consent should be understood in line with the requirement in article 4.3 of Council Decision 2000/642/JHA of 17 October 2000[134].

44. **Strict adherence to the principle of availability** under different sources such as the Hague and Prüm treaty[135] and the Council framework Decision 2008/977/JHA[136], and the drive to respect the CDD obligations by international or global institutions in the most cost effective way, the centralisation or even globalization of available information (KYC, CDD and STR data) or risk management **contradicts several fundamental data protection principles**[137]. In particular, it leads to an increase in the risk of ineffective processing with inaccurate, obsolete and uncontrollable data and without fully satisfying data protection as required by national and EU data protection laws. For effective data protection, WP29 is instead of the opinion that local storage of AML/CFT data within the EU or countries with adequate data protection should be required and made subject to regular compliance checks with the applicable national data protection laws. Those checks should be readily available and documented in the internal DP compliance policy (see above).

133 See page 42 nr. 100 of the final report of LRDP Kantor Ltd and Centre for Public Reform

134 Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000, p. 4–6

135 Prüm already challenged and toned down the Principle of availability promoted by the Commission in the Hague Programme

136 See recital 5 of this decision

137 See n° 30 of the final report of LRDP Kantor Ltd and Centre for Public Reform