



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

Adopted on 13 June 2011

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

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

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

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

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

having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,

having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

1. INTRODUCTION

During its plenary meeting of today, the Article 29 Data Protection Working Party ("**Working Party**") has issued 44 recommendations concerning privacy and data protection related to the prevention of money laundering and terrorist financing ("AML/CFT"), attached in annex to this opinion.

2. CONTEXT AND AIM OF THE 44 AML/CFT RECOMMENDATIONS

Prior to the adoption of these recommendations, the Working Party consulted different stakeholders, including but not limited to the European Commission, representatives from reporting entities, financial intelligence units, national banks and the FATF. This to make sure that all relevant data protection and privacy issues that were raised by these actors were investigated in the light of the existing legal framework on privacy and data protection.

The recommendations intend to give a position and practical guidance to legislators, reporting entities, regulators, Financial Intelligence Units, supervising authorities and other stakeholders that are called upon to apply principles and regulations in both areas to the prevention of money laundering and terrorist financing as well as privacy and data protection at EU as well as national level.

These recommendations address the need for practical and broad guidance at the level of the European Union in the combined area of the prevention of money laundering and terrorist financing as well as privacy and data protection (explained in point 1.4 of the annex).

3. MAIN CONCERNS

The recommendations address different concerns (point 1.5 annex). The main ideas that are addressed in the recommendations are:

- * Privacy and data protection are established within the EU as a human right as part of a democratic society *according to law (article 8 ECHR)*, and should always be applied as such rather than on the grounds of legitimate interest or the consent of the data subject (rec. 1). Hence, measures that are imposed as obligations to prevent money laundering and terrorist financing should always have a clear legal basis and remain necessary and proportionate to the nature of the data. The WP29 recommends a.o. a review of current and proposed AML/CFT laws at EU and national level (rec. 3), more EU harmonization (rec. 5); readable public data protection policies (rec. 12), clear information for visible AML/CFT measures such as questionnaires and the limitation of services (rec. 13), and the strict and clear application of the purpose limitation principle in AML/CFT laws (rec. 15-16).
- * The principles and obligations in this area should be dealt with *in a balanced way*, taking into account the different opinions, interests and legal framework in the EU and beyond. Examples include the redaction of AML/CFT laws and guidance (rec.2), the use of prior data protection assessments (rec. 7-9), the balanced use of feedback (rec. 22), the avoidance of goldplated AML/CFT regulations (rec. 23), balanced data sharing schemes (rec. 26), a balanced view on data retention mechanisms (rec. 28), a balanced view of the prohibition of tipping off that respects data protection rights (rec. 12-13)
- * Privacy and data protection rights and obligations should always be addressed and developed in this area *in a positive way*, rather than referring to privacy and data protection in a negative way. Examples of negative approaches are to present privacy and data protection as an obstacle that can or should always be circumvented, and the approach that is limited to the blanket application of exceptions to data protection legislation, ignoring the conditions for such exceptions, and offering in return no real content and substance to privacy and data protection in the context of AML/CFT processing. The idea of a positive approach is illustrated a.o. by the recommendations that concern specific measures such as the adoption of public and documented privacy and

data protection compliance policies by reporting entities, FIUs and financial supervisors (rec. 11), internal, confidential data protection policies (rec. 14), the prevention of identity theft (rec 38), the use of FIU disclaimers for the use of typologies (rec. 19) and feedback mechanism (rec. 21), the provision of appropriate safeguards for every profiling operation (rec 20.), continuous data accuracy assessments (rec. 29) the storage of data source and date for all AML/CFT data and assessments (rec. 30), access and supervision via DPAs (rec 34) and the protection of sensitive data (rec. 37)

- * ***WP29 recommends that in order to offer real, effective protection*** and compliance with privacy and data protection in this field, application of different forms of prior assessment of AML/CFT laws, procedures and projects should be undertaken. Such forms include privacy impact assessments, auditing techniques, the work of data protection officials,... (rec. 7-10). Also recommended are quality assessments such as BCR stress tests for institutions that wish to adopt BCRs (rec 39), the required benchmark for adequacy findings for international transfers (rec. 40), and the use of MOUs by FIUS as tools for data protection (rec 43).

- * ***Continued and improved cooperation*** amongst different stakeholders is required in order to ensure legal certainty at EU level, including the different supervising authorities such as DPAs, FIUs and Financial Regulators (rec 17)

4. CONCLUSION

The Working Party 29 will follow up the attached recommendations and the relevant developments in legislation and practises in the combined area of the prevention of money laundering and terrorist financing as well as privacy and data protection.

Done at Brussels, on 13 June 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM