Brussels, 28 April 2008

EU FINANCIAL INTELLIGENCE UNITS' PLATFORM

REPORT ON

CONFIDENTIALITY AND DATA PROTECTION IN THE ACTIVITY OF FIUs[1]

(Good practices)

The EU Financial Intelligence Units' Platform was set up in 2006 by the European Commission, which participates in its activities and provides support. The main purpose is to facilitate cooperation and exchange of information among FIUs of EU Member States, with a view to identify problems and good practices in the framework of the implementation of the third EU AML/CFT Directive.

[1] This report has been prepared by the EU FIU Platform on the basis of groundwork carried out by representatives of the FIUs of Belgium and France, with the support of the European Commission, taking account of information provided directly by 7 members of the thematic working group on "Confidentiality and Data Protection" of the Platform.

Table of Content

The aim of the report is to identify any convergence points and any conciliation difficulties between legislation on the fight against money laundering and terrorism financing on the one hand, and legislation on personal data protection on the other.

1. CURRENT SITUATION

In conformity with Directive 95/46 /EC of 24 October 1995, all countries have legislation on personal data protection in place; they also have a supervisory authority in this field, entrusted with ensuring compliance to legislative provisions, which has the appropriate powers (on-site check, sanctions including penal ones, whose generalisation at European level would be suitable for the actions of supervisory authorities).

	Reference document	Supervisory authority
Belgium	Law of 8 December 1992 amended by the law of 11 December 1998	Belgian privacy protection commission
Denmark	Act. No. 429 of 31 May 2000	Data Protection Agency
Spain	Organic law 15/1999 of 13 December 1999 Royal decree 994/1999 of 11 June 1999	Spanish Agency for Data Protection
France	Law of 6 January 1978 amended by the law of 6 August 2004	French national commission for data protection and the liberties (CNIL)
Latvia	Natural person data protection law, adopted in 20th April, 2000	State Data Inspection
Luxembourg	Law of 2 August 2002. A draft law no. 5554 amending certain provisions of this law is about to be adopted by the Chamber of Deputies.	National data protection authority
Portugal	Law No. 67/98, of 26 October 1998	National Committee for Data Protection

1.1. DATA PROCESSING CARRIED OUT BY FINANCIAL INTELLIGENCE UNITS

The mechanisms for fighting money laundering and terrorism financing require personal data processing by financial intelligence units.

In general, the latter are subject to prior report/notification to the national supervisory authority. This report defines the objective of data processing (fight against money laundering and terrorism financing) and also the authorities/services, foreign financial intelligence units in particular, which are authorised as recipients of data collected as stipulated by the relevant national legislation on the fight against money laundering and terrorism financing.

Sensitive data

In principle, legislation on personal data protection prohibits personal data collection that reveals racial or ethnic origin, political, philosophical or religious opinions or trade union membership or data concerning health or sex life. However, a number of exceptions have been foreseen provided the objective of processing justifies the input of such data.

Data processing for Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) purposes is in itself legitimate provided it derives from a law and that processing of specific data appears to be justified within this framework (political or religious terrorism, organised crime, channels, networks and typologies). In order to sustain guarantees in terms of data protection, the principle of prohibition of processing such sensitive data is imposed; nevertheless, it would be convenient for FIUs to be allowed to process data that is considered particularly essential within the framework of their fight against terrorism financing. This task does not give rise to particular constraints for FIUs in terms of confidentiality given that the latter ensure the security of their data.

In addition, both Directive 95/46/EC and the Proposal for a Council Framework Decision on the protection of personal data allow exemptions to the principle of processing sensitive/specific data for reasons of substantial public interest (Directive) or when this is strictly necessary (Framework Decision) and when appropriate safeguards are provided for by national law.

As part of the prior notice, the data protection authority should receive the details of the specific data that are processed, the list or categories of persons that have access to these data and a duty of professional secrecy for these persons, as well as the right to indirect access to personal data by means of the supervisory data protection authority referred to below.

Individual's rights with regard to the processing carried out by Financial Intelligence Unit

In conformity with European Directive 95/46/EC, European legislation foresees a number of rights for individuals with respect to the processing of nominal data such as:

- the right to information: if the data is not collected from the person concerned, the latter shall be informed of the conditions of use of such data and their rights upon recording of such data or upon their first disclosure;

- right of access: all individuals may, free of charge, have access to all information concerning them, in accessible format, by submitting a simple application to the relevant organisation and, if necessary, obtain a copy thereof;

- the right to rectify any data concerning an individual is associated with this right of access.

These principles are inconsistent with the confidentiality requirements associated with the actions of FIUs. Moreover, processing carried out by FIUs, generally speaking, benefits from relevant derogation measures that vary from simple exclusion from these rights (for judicial FIUs in particular) to limitation of their scope.

Exclusion from the right to information: the granting of such a right would be particularly contradictory with pursued objectives as it would oblige the FIU to inform the person concerned that a suspicious transaction report concerning them has been integrated in a data processing exercise whose objective is to combat money laundering and terrorism financing. This would not only be contrary to the efficiency of the fight against money laundering and terrorism financing but would also affect the fundamental principles in this field, applicable to both the FIU and professionals, that prohibit any disclosure of the existence of a suspicious transaction report to the person concerned.

No right of access but indirect access

The right to indirect access is exercised by the supervisory authority intermediary: individuals should refer to the supervisory authority requesting it to proceed with the verification of information concerning them that might be recorded in this type of file. Subsequently, the authority notifies the applicant that it has carried out verification without providing any further information.

The implementation of such restrictions on the access of individuals to FIU databases is essential: the report of suspected of money laundering or terrorism financing to the intelligence unit benefits from a very high level of confidentiality arising in particular from a wish to ensure the protection of the identity of the reporting party and avoid the latter becoming the victim of attacks or reprisals. Thus, granting a right of direct access to defendants would be contrary to the requirements of protecting the anonymity of the disclosing source and would fundamentally call into question the mechanism for combating money laundering and terrorism financing. That would

lead, as in the case of the right to information, to circumvention of the “tipping off” prohibition on the basis of legislation on personal data protection.

Such derogation measures (right of information, access and rectification) appear to be a good compromise in order to avoid hindering the fight against money laundering and terrorism financing and, within this framework, ensuring that the type of data protection is suitable for the context of processing.

In this respect both Directive 95/46/EC (article 13) and the proposal for a framework decision (article 16 and following) on data protection offer the possibility to restrict the rights of a person whose data are being processed, a.o. in order to safeguard national security or to avoid harming crime prevention. The latter legitimizes specific measures required for AML/CFT purposes. In the framework of data exchange between Member States it is stipulated that each Member State may request another one not to inform the individual involved. This is well balanced with the limited scope of this exemption as well as with the supervision of the data protection authority through its right of indirect access.

Statistical data

The objective of statistical data processing is limited to evaluating the efficiency of the national instrument for fighting money laundering and terrorism financing. Thus, according to FATF recommendations, the issue consists in elaborating typologies that will facilitate the detection of laundering transactions, in such a way that this processing targets the same objectives as basic processing carried out for the purpose of fighting money laundering and terrorism financing. In this respect, it does not appear necessary to obtain subsequent consent from the supervisory authority.

Under both Directive 95/46/EC and the proposal for a framework decision this kind of "reprocessing" is not considered incompatible with the initial processing provided that MS lay down appropriate safeguards, e.g. anonymisation of information used or processed to do statistics and appropriate security measures such a restriction access to data to avoid identification of persons, etc.

Statistics per definition involve the processing of information on an aggregate manner. The information collected for statistics is worked out in such a way that it cuts the link between that information and the individual behind the information. Measures are taken to impede traceability backwards of individuals (anonymisation). Article 33 of the AML/CFT Directive (2005/60/EC) provides for the obligation to maintain appropriate statistics, with "aggregate information" on the activities of FIUs. The purpose is to know how many cases have been investigated or how much property has been frozen or seized, not whether Mr. X has been investigated or his property seized. This statistical information shall not allow FIUs to identify individuals.

This section of the document refers only to "statistics" strictly speaking and so does not seem to pose any problems with respect to data protection.

With regard to the consent, as Article 33 of the AML/CFT Directive provides a legal basis for the establishment of statistics, and this processing could be considered as justified by an objective of public interest, there does not appear necessary to obtain

the prior consent of individuals. However this does not imply that, when personal data is collected from the data subject, the financial institution (bank, lawyer, etc.) provides the data subject with the appropriate information and informs him/her on the fact that his/her personal data may be used for statistic purposes.

Data storage period

Data storage periods vary from country to country: variable time limit, (DK, PT) or predetermined period (LV, FR). Countries in which no period has been set have begun discussions on this issue (BE, LUX).

One of the difficulties arises from the fact that an individual can be the object of successive reports submitted to the FIU, which poses the problem of defining the start date for the data storage period.

In any case, considering the fluctuating nature of the data that FIUs are expected to process, it would be suitable for their data storage period to begin when a new piece of information is communicated to them about the person concerned.

The data retention period is a basic element of the processing of personal data. Personal data which reaches the retention period imposed by a legal act are to be erased or archived separately and may not be longer processed, unless that data is being processed in the context of an investigation which is still open.

Accordingly, "old data" contained in a personal file shall be erased or not longer processed when they reach the retention date fixed by the national law applicable to the entity processing this personal data, except if that data is being used in an investigation.

When establishing a national storage period for data processed by FIUs the judicial use of information processed by FIUs should be taken into account. The prescription term applied for criminal proceedings could be a useful point of reference to define the maximum storage period. An extension beyond this period might then require a periodical evaluation to assess whether it is necessary to keep these data in the active database.

A different approach should be used on the one hand for data included in files forwarded to the judicial authorities, which should be treated like data from judicial files, and on the other for data from files that were closed by FIUs. The latter should be stored during a limited period of time in order to assess the necessity to keep them or not.

Moreover, the question of reconciling different storage periods is also posed within the framework of operational cooperation between FIUs. Should the period applicable with respect to personal data be that of the country of origin of the information or the period applicable in the receiving country?

➢ The relevant provisions of the examined bilateral cooperation agreements lack uniformity, within the EU and with third countries too. Data benefit from the protection accorded to similar information by the national legislation of the competent authority receiving the data or providing it, accordingly, which is a source of insecurity as regards personal data protection.

Bilateral agreements should make efforts to define the rules governing the data storage period within the framework of information exchanges between FIUs and seek inspiration from the Egmont Group cooperation agreement model.

This situation implies that FIUs should be aware of one another's data storage period. This could partly be resolved by a reference in the bilateral memorandum of understanding between both parties or by specifically mentioning this when data are being transferred.

➢ At European level, it is important to note the draft framework decision for data protection in police and justice matters which recently reached political agreement, and which includes a specific article on the issue. Article 10 of this draft decision states that the transmitting authority may upon transmission indicate the time limits for the retention of data, following the expiry of which the recipient must also erase or block the data or review whether or not they are still needed. This obligation shall not apply if, when these time limits expire, the data are required for a current investigation or prosecution. When the transmitting authority refrained from indicating a time limit, the time limits for the retention of data provided for under the national law of the receiving Member States shall apply.

This provision provides relative flexibility but imposes reciprocal knowledge by European financial intelligence units of their respective data storage deadlines.

For instance, sending the information from a FIU to another FIU which has a longer retention data in its national law and some time later request that information in order to start a new processing activity shall be fraud.

Data contained in files closed within FIUs

Data contained in files closed within FIUs must be kept for a period of time that allows to assess them in the light of any subsequent information forwarded with respect to the same transaction or the same individual. This period for storing data should be defined. In this regard it should be specified that the data storage period starts over when the FIU receives new relevant information.

Even though all data in disclosures are processed by FIUs, it should be granted that data received at time "t" may not be the object of immediate use in a file reported to the judicial authorities but may take on a totally new dimension in the future on the basis of further information.

Erroneous data

Personal data need to be *accurate and relevant and kept up to date*. An erroneous personal data contained in a personal file means an erroneous processing activity

which would not be in the interest of the data controller. Therefore, it is in the data controller's interests as well as the data subject's interest that erroneous personal data shall be corrected as soon as it appears that personal information is erroneous.

Erroneous data requires then immediate rectification from the point of view of legislation on data protection on the one hand and guaranteeing the reliability of the data base on the other.

Protection of data confidentiality by the FIU

With respect to this, there is perfect convergence between the two types of legislation given that, in application of both, FIUs are required to ensure the security of data processed within their service and that processing possibilities are limited to what people need in order to exercise their duties or to what is necessary for the requirements of the service.

Confidentiality is not an obstacle to derogations given that recipients of data are clearly identified and that information transmission is justified only for AML/CFT purposes (judicial authority, foreign FIU counterparts, or other national services).

1.2. PERSONAL DATA PROCESSING AND PROFESSIONS SUBJECT TO THE MECHANISM FOR FIGHTING MONEY LAUNDERING AND TERRORISM FINANCING

Implementation of specific processing related to the application of their obligations to fight money laundering and terrorism financing

Professions subject to the mechanism for fighting money laundering and terrorism financing have full power to define the means for fulfilling their relevant obligations, which may be based on personal data processing.

This targeted processing for fighting money laundering and terrorism financing purposes also tends to take place within the framework of the risk-based approach foreseen by the third AML/CFT Directive.

As mentioned before, Directive 95/46/EC as well as the proposal for a framework decision on data protection allow in some cases to restrict the rights of a person whose data are being processed. Based on this the AML/CFT Directive already contains a basic rule (Article 28) which obliges professions covered by that Directive not to disclose to the customer or other third person (for instance customer's lawyer) that fact that information has been transmitted to FIUs or that an investigation is being carried out or may be carried out. Therefore there is no “conflict” between these two legal acts.

This question is different from whether these professions must inform their customers at the time they collect the data, or whether there is a right of access that can be carried out indirectly by means of the national data protection authority. It is not evident that all banks properly inform their clients of the fact that the personal data

they collect shall be processed for the purposes of the fighting money laundering and financing terrorism and that, in this context, the data can be disclosed to other entities competent for this purpose (FIUs as well as to other entities of the group as provided in article 28 of Money Laundering Directive). It has also to be reminded that all these data processing activities remain subjected to the supervision of the data protection authorities and national data protection laws. Article 28 may justify denying direct access to personal data to a data subject. However the fact that direct access is not granted does not mean that an indirect access to personal data processed by FIUs may not be granted either. The question here is how this right of access should be organised in order to strike different interest at stake. Several national laws provide for an indirect access by national data protection authorities to the data processed by FIUs. The recent Framework Decision on the protection of personal data in the third pillar refers to this indirect access in its recital 14a. This indirect access shall in any case be granted, also within the financial institutions.

The current legal framework, as laid down in the AML/CFT Directive, namely article 28, already strikes the appropriate balance between the legitimate concerns posed by combating money laundering and terrorist financing and the protection of individuals. The derogations provided are sufficient.

However, a risk of leaks remains. This should be taken into account and it should be recalled that personal data collected for AML/CFT purposes may not be further processed for other purposes unless there is an appropriate legal basis, in particular to avoid customer risk management from a purely commercial point of view.

Nature of files to which professions may have access for facilitating the fulfilment of their due diligence obligations

Disclosing professions have access to various open databases but not to that of the FIU and, in principle, not to files kept by other national services.

Although access to certain files would be of interest to professionals within the framework of the fulfilment of their AML/CFT obligations, the relevance of a global move aiming at offering professionals access to increasingly large databases, beyond any effective control providing sufficient guarantees as regards data protection and further use of such data, should be questioned. In any case, the FIU's data itself should remain inaccessible to professionals.

2. USE AND EXCHANGE OF DATA BY THE FIU

Compliance with the principle of purpose

At national level, conformity of AML/CFT systems with legislation on data protection implies respect for the purpose of data processing carried out within this framework i.e. fighting money laundering and terrorism financing. Data collected and processed by FIUs cannot thenceforth be used for other purposes, unless explicitly authorised by national law.

However, the proposal for a framework decision on the protection of personal data allows, under certain conditions, that data is later processed for other purposes, when this is not incompatible with the purposes for which the same data were collected. Competent authorities are allowed to process these data in accordance with the applicable provisions and when this is necessary for and proportionate to these purposes. Reference should also be made to article 12 of this proposal, which indicates that in some cases personal data exchanged between Member States may later be processed for other purposes than those for which they were transmitted, such as the prevention and detection of criminal offences. In the same context, one should also refer to article 13 of Directive 95/46/EC. AML/CFT legislations seem to be more restrictive on this issue.

In contrast, this principle of speciality does not apply in exchange between FIUs and judicial authorities that have full jurisdiction in terms of criminal proceedings. On the other hand, the fact that judicial action cannot be limited ensures prosecution of defendants for the underlying offence even if the laundering crime cannot be qualified at the beginning of judicial investigations carried out on the basis of information from the FIU.

Exceptions to the confidentiality principle

Other derogations could be foreseen, the most important of which concerns the exchange of information between FIUs.

FIUs are enabled to cooperate with counterpart units that fulfil similar functions and are subject to the same secrecy and confidentiality rules. Prior consent is needed for further use of the exchanged data and their transmission to third parties.

The provision of an adequate level of protection of personal data is a requirement for the receiving FIU.

At European level, Council Decision 2000/642/JHA of 17 October 2000 sets out arrangements for the cooperation between FIUs of the Member-State, also as regards the protection of data transmitted within this framework. The exchanged information must be protected by at least the same rules of confidentiality and protection of personal data as those that apply under the domestic legislation of the requesting FIU.

This decision acknowledges exceptional circumstances in which an FIU may refuse to divulge information, i.e. when this could lead to impairment of a criminal investigation being conducted in the requested Member State or where divulgation of the information would otherwise not be in accordance with fundamental principles of national law and would be clearly disproportionate to the legitimate interests of a natural or legal person of the Member State concerned.

For exchanges of information with third countries, this matter is regulated by each State within the framework of bilateral cooperation agreements. These agreements allow for a case by case cooperation consistent with EU data protection rules.

Principle of adequate level of protection

For third countries, personal data protection legislation should foresee that the country in which the data is to be processed ensures an adequate level of protection with regard to personal data. Nevertheless, the difficulty resides in the practices that are not yet harmonised with respect to this principle.

In general, the confidentiality regime applicable to the information exchanged is equivalent, thus allowing the cooperation to be carried out.

Also, the definition of "Memoranda Of Understanding" (MOU) with a large number of foreign FIUs ensures that the cooperation is in conformity with the protection of privacy.

The provisions on data protection applicable to data transfers to third countries allow for exceptions concerning the adequate level of protection when important public interests prevail. AML/CFT can be considered as such an interest. This being said the Egmont Group model MOU imposes strict confidentiality for information sharing, requiring consent among parties as regards further use of the data.

Principle of prior consent

In general, the use of the information transmitted through cooperation between FIUs is subject to prior consent from the FIU from which the information originates. This is also a guarantee for data protection.

This need of a prior consent can be regarded as a fundamental principle in this field, as it is also provided for in the draft framework decision on data protection in the field of cooperation in police and justice affairs.

However, various practical issues arise with respect to the scope of this consent.

➢ When the information originates from another national authority and, in particular, if such information concerns sensitive or specific data.

With respect to this, the rule to be imposed should consist in obtaining, via the national FIU, prior consent from the service providing the data.

➢ Is the authorisation granted only valid for the specific case described in the application or does it have a general scope thus permitting any further use of the data by the receiving FIU?

Consent on a case-by-case basis undoubtedly provides more guarantees with respect to data protection given that such a procedure not only allows for verification that the data remains precise and is not deleted in the country of origin but also for ensuring that anticipated future use is in conformity with the legislation of the State transmitting the information.

This new processing could be allowed in certain Member States as part of the measures taken at national level for purposes of crime prevention. This "change" of finality of the processing should be made subject to the consent of the communicating FIU.

➢ Future use of the data originating from a European counterpart for informing a third party FIU.

The prior consent principle of the transmitting FIU once again appears to be necessary in order to provide a maximum of guarantees as regards data protection. But it also appears essential to request the third party FIU to contact the FIU that is the holder of such information in view of obtaining this consent, both for avoiding circumvention of existing bilateral cooperation agreements between the two countries and for adhering to respective national legislation on data protection.

➢ The use of information transmitted between Member States that do not have the same approach to the money laundering offence (especially in relation to the scope of predicate offences, be it based on a "all crimes" approach or on a list of offences).

It seems that in such situations the requested Member State may specify the scope of its consent by indicating any restrictions in this regard.

➢ The use of information exchanged between Member States to be transmitted to third parties or private individuals

The proposal for a framework decision on data protection allows this type of transfers, through prior consent of the authority providing the information, as part of crime prevention and if no specific legitimate interest of the individual involved prevents the transfer. However Council Decision 2000/642/JHA requires that FIUs undertake all necessary measures to ensure that shared information cannot be accessed by any other authority, agency or department. In general, confidentiality and professional secrecy prevent FIUs from transmitting such information.

However, the provisions of the proposal for a framework decision on data protection are minimum requirements and the system applicable to FIUs is more restrictive, even though it has to be acknowledged that there is no clear definition of "third parties". In particular, transmitting data to other authorities raises issues.

However, as regards this subject, one should refer to the Egmont Group model MOU, used by most FIUs:

- free exchange of information on condition that the information provided is exclusively used internally by the receiving service;
- no other use of data exchanged is permitted without explicit prior consent from the transmitting service;
- exchange of information subject to strict confidentiality unless otherwise provided by common agreement.

This model could be further refined in order to obtain a more uniform framework as to the content of the provisions that should be implemented in this regard.

FIUs access to other national files

Direct access to files managed by other national services, without being the object of reciprocity, reinforces the efficiency of FIUs' action in fighting money laundering and terrorism financing. It might prove decisive for convincing an FIU of the existence of serious indications of money laundering or terrorism financing. The data protection authority should however be able to ensure control of the processing of data originating from such files and/or validate access to them.

This is a sensitive issue. FIUs' direct (or indirect) access to data files managed by other national services implies a further processing of this personal data for a purpose other than that for which the data has been collected.

It means a change of purpose of the processing. Such an access needs to be justified under an appropriate legal basis in accordance with national law.

However, unless consent is granted by the national service providing the data, the FIU does not have, in principle, a right to forward that data to third parties, including foreign FIUs

National provisions could simplify this system, for example allowing the transfer of data obtained from another national service without its prior consent to counterpart FIUs which offer adequate guarantees with respect to data protection.

Feedback to disclosing professions

It is essential to inform disclosing parties of the types of transactions requiring additional diligence and of developments observed concerning money laundering or terrorism financing techniques to which criminals resort. Moreover, reporting sectors are further motivated if they are informed about the actions carried out as a result of their reports. On the other hand, the AML/CFT Directive requires Member States to ensure, where practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing.

Although general information does not appear to pose particular difficulties for data protection, the same does not apply to information on follow-up to reporting of particular suspicious transactions.

In fact, it has been confirmed that a number of professionals misuse such information by using it for customer risk management and for terminating contractual relations with the person concerned, which not only affects the respect of the individual’s rights but also the efficiency of the fight against money laundering and terrorism financing (at all stages of the investigation).

Such *impromptu* terminations of business relationships cannot but alert the money launderer or terrorism financier to the fact that they are the subject of a report submitted to the FIU. This also implies a change of purpose of the information communicated which, as such, would be illegal and in conflict with national data protection law.

Moreover, this aspect will be amplified by the exceptions to the tipping off prohibition, foreseen by article 28 of the AML/CFT Directive, which allows circulation of information within the same group of financial institutions or network of professionals.

In general, the scope and extent of exchange of information with the private sector is an issue. A too wide sharing of the information collected by FIUs may pose relevant problems as regards professional secrecy and data protection.

3. SHARING WITHIN THE SAME GROUP

Article 28 of the AML/CFT Directive, while reaffirming the prohibition of "tipping-off", allows for the circulation of information on suspicious transactions within the group or professional network, under certain conditions.

In particular, it is required that the institution or the person to whom the information are communicated be subject to equivalent obligations with respect to professional secrecy and data protection and that any information exchanged be used exclusively for purposes of money laundering or terrorism financing prevention.

Although such derogations satisfy the need to reinforce the fight against money laundering and facilitate within groups the integration of the risk-based approach logic, they raise a number of matters of principle, from the FIUs' point of view, as regards professional secrecy and confidentiality, the principle of territoriality, the cooperation between FIUs, data protection, the secure feedback of information to disclosing professions.

Protection of personal data rests, in particular, on the central role played by FIUs. Those are subject to professional secrecy obligations which ensure, on the one hand, that the information received is kept confidential and, on the other hand, that such information only flows in one direction, that is from disclosing parties to the FIUs themselves and to other FIUs, provided that they are subject to similar professional secrecy and data protection obligations. The possibility of sharing information on suspicious transactions within a group or a network of professionals constitutes an exception to this regime and brings the risk that such information is circulated in an unsafe way.

Thus, from the FIUs point of view, there is a need to strike the right balance between contradictory objectives and to regulate those measures that can affect the right of privacy and personal data protection in a suitable way.

Although the exceptions to the “tipping off” prohibition introduced by the AML/CFT Directive is accompanied by guarantees (they are allowed only for fighting money laundering and terrorism financing purposes; they are only possible if the recipient is subject to equivalent obligations with respect to professional secrecy and personal data protection), the question of how to ensure respect for these principles and avoid the use of the information for commercial management of customer-related risks remains open. In practice, where information is circulated within a group or a professional network, one has to take into account the purpose of this circulation. Therefore it is necessary to ensure that only those persons who are responsible for AML/CFT may have access to such information and that it is only used for these specific purposes. Appropriate organizational and technical measures should be implemented to ensure compliance with these principles.

Moreover, other problems might arise with respect to data protection.

➢ The content and the format of the information exchanged remains uncertain and the same applies to the existence of measures for protecting the reporting parties themselves. The growing number of persons that might need to know about the existence of a report of suspicious transactions and the consequent exposure of the person that submitted the report inherently constitute risk factors. This is particularly true if such information is accessible in a third country that does not have anti-money laundering legislation in place nor legislation on personal data protection offering sufficient guarantees.

➢ With regard to the circulation of information to entities located in a third country, the principles relating to international data transfers apply both with respect to data protection and AML/CFT legislation. This requires an adequate level of data protection, which can be lowered in order to allow data transfers necessary to safeguard an important public interest and a prior consent of the Member State supplying the data in case these were transmitted between Members States before. There is a risk of external leaks in case of lack of control on the transmitted data. See in this regard recital 33 of the AML/CFT Directive: "Disclosure of information as referred to in Article 28 should be in accordance with the rules on transfer of personal data to third countries as laid down in Directive 95/46/EC".

➢ Article 28 of the AML/CFT Directive maintains the prohibition of tipping-off, which prevents the reporting entities to inform their client that information was transmitted to the national FIU. Yet Member States should ensure that this provision is strictly applied in order to avoid any mistakes in this regard.

The screening imposed by the applicable European legislation does not totally exclude that a potential money launderer would go to his bank agency to check the data available at domestic level but also the data held abroad by institutions of the same group and through the configuration of this file. This risk is higher in countries whose AML/CFT system is less developed.

The right of information is restricted, as explicitly provided for in the AML/CFT directive, but also the right of access, taking into account the purpose, that is the prevention of money laundering and terrorist financing (see articles 13 of the Directive 95/46/EC and 16-17 of the proposal for a framework decision on data protection).

This is a potential risk that requires appropriate structuring of the group and a division of the services involved in order to avoid any mistakes.

➢ Furthermore, parallel channels of information exchange are likely to be created outside the framework of official secured mutual cooperation between FIUs given that an FIU might obtain information from the national branch or subsidiary of a group that has obtained such information within the framework of intra-group exchanges with entities abroad.

There is a risk of duplicating the FIU's work in this regard. The principle of territoriality related to the transmission of suspicious transaction reports could accordingly encounter difficulties with respect to its application due to possible centralisation of reports of suspicious transactions within the parent companies of groups.

➢ Data transfer could also take place with authorities other than FIUs despite rules applicable to money laundering and terrorism financing matters.

One cannot exclude that sharing of information within the same group with respect to individuals suspected of money laundering or terrorism financing might lead to subsequent transfers to other authorities than those competent in the field of AML/CFT, in a way that might be inconsistent with data protection measures.

➢ Finally, there is also the risk that some professionals might use the sharing of information within the same group to circumvent the prohibition to provide information following a request by the judicial authorities. So sending a disclosure to the FIU containing the same information would allow this information to circulate anyway.

- Discussions are being held currently concerning the elaboration of a list of countries that could benefit from the recognition of an equivalence presumption in law, on the basis of FATF criteria, with particular regard to the implementation of Article 28 of Directive 2005/60/EC. This appraisal cannot be limited to the AML/CFT criteria only, but should also include the consideration of the adequacy of personal data protection in the third country concerned, especially by referring to the work of the “data protection” group known as "Article 29 working party").

- In any case, extended cooperation does not seem to offer real guarantees in the field of data protection. It would be useful to favour data exchanges via FIUs offering safe channels as regards data protection and to strictly regulate circulation of information between the same group in order to avoid different interpretation and excessively widespread dissemination of data that is beyond any control. Harmonisation of provisions regulating such exchanges would also offer better guarantees as regards data protection.