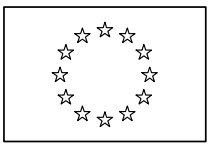

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 29.11.2005
COM(2005) 620 final

COMMISSION COMMUNICATION TO THE COUNCIL, THE EUROPEAN PARLIAMENT AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

The Prevention of and Fight against Terrorist Financing through enhanced national level coordination and greater transparency of the non-profit sector.

INTRODUCTION

Preventing terrorists from gaining access to financial resources is one of the cornerstones of the EU's fight against terrorism. This is highlighted in the Action Plan on Combating Terrorism[1] and the Council Declarations following the attacks in Madrid and London[2]. EU policy in this area was further set out in the Commission Communication of October 2004[3] and the EU Counter Terrorist Financing Strategy of December 2004[4]. These make clear that the importance of this work is not only to prevent terrorists from gaining access to funding but also to maximise the use of financial intelligence in all aspects of counter terrorist work.

In its Declaration on Combating Terrorism of 25th March 2004 the European Council called on Member States "to increase cooperation between national competent authorities, Financial Intelligence Units, and private financial institutions to facilitate improved exchange of information on terrorist financing"[5]. The Declaration also called on the Commission to consider improvements in the regulation and transparency of non-profit organisations ("NPOs") which may be used by terrorists to acquire funding for their activities. This Communication addresses these core elements in the fight against terrorist financing. Part I assesses national level coordination issues. Part II deals with vulnerabilities of the non-profit sector to terrorist financing and outlines a Recommendation for Member States and a Framework for a Code of Conduct for NPOs contained in the Annex to this Communication.

PART I - NATIONAL COORDINATION STRUCTURES

The Peer Evaluation on terrorism ("National anti-terrorist arrangements: improving national machinery and capability for the fight against terrorism")[6] has proved a valuable tool in helping Member States to assess their national counter-terrorism arrangements. The fight against the financing of terrorism was within the scope of the Peer Evaluation. The enormity of the task has meant that country reports and recommendations have not always addressed the financing of terrorism in particular detail. Consideration should therefore be given to focusing on national machinery addressing the fight against the financing of terrorism and drawing on findings set out in this Communication as a possible topic for a follow-up Peer Evaluation.

---

1 Plan of Action on Combating Terrorism 10586/04 of 15th June 2004 (Council Document)

2 Declaration on Combating Terrorism adopted by European Council 25th March 2004; Council Declaration on EU Response to London Bombings adopted by Extraordinary Council meeting (Justice and Home Affairs) 13th July 2005.

3 Commission Communication on Prevention of and Fight against Terrorist Financing 20.10.2004 COM(2004) 700

4 « The fight against terrorist financing » presented by Secretary General/High Representative and Commission to European Council. 16089/04 of 14th December 2004 (Council Document)

5 Recommendation 31 of the Financial Action Task Force Forty Recommendations calls on countries to ensure that "policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing".

6 Following the 11th September 2001 attacks the JHA Council of September 2001 launched an assessment of national anti-terrorist arrangements.

The Hague Programme states that the mere fact that information crosses borders should no longer be relevant in the EU[7]. An effective exchange of information between competent authorities in the EU is, however, dependent on comprehensive and effective national level coordination to identify, cross reference and analyse relevant information and produce reliable high quality criminal intelligence. Well coordinated national level information exchange is essential if the "principle of availability" [8] is to operate effectively since, in the absence of appropriate national level coordination and generation of high quality criminal intelligence, information/intelligence sought at EU level may not be available.

The EU Counter Terrorist Financing Strategy invited the Commission to assess national coordination structures between different Ministries, agencies and other actors engaged in counter financing of terrorism ("CFT") work. It invited the Commission to consider possible additional cooperation methods between law enforcement/intelligence services and the private sector. The Commission's analysis is largely based on Member State answers to a questionnaire sent to the EU 25 in mid-March 2005 as well as discussions with Europol and industry representatives.

In replies to this questionnaire Member States confirmed that State bodies engaged in the fight against financing of terrorism include Finance, Justice, Interior and Foreign Ministries, Treasury Department as well as the Financial Intelligence Unit, specialised financial police, Public Prosecutor's Office, Customs Authorities, Tax Revenue Services, intelligence services, financial regulators and the Central Bank ("Relevant Actors").

The advantages of ensuring coordination among Relevant Actors were highlighted by many Member States:

> "…representatives of the majority of competent bodies meet in one place and directly exchange relevant information, assess it and elaborate the final product for the decision-makers based on consensus. The brain-storming that evolves during such direct meetings of experts is particularly useful as well as the possibility to deal with individual issues in an all-encompassing manner."[9]

Coordination and information sharing among national agencies were highlighted in the Council's best practices paper on financial restrictive measures targeting terrorism[10]. The analysis set out in this Communication is compatible with and should supplement this approach.

---

7 The Hague Programme: strengthening freedom, security and justice in the EU. Brussels 13th December 2004 16054/04 (Council Document). See also the Proposal for a Council Framework Decision on the exchange of information under the principle of availability COM(2005)490 of 12.10.2005

8 See The Hague Programme Section 2 on improving the exchange of information for law enforcement purposes.

9 Reply to Commission questionnaire provided by Permanent Representation of the Republic of Slovenia to the European Union

10 Council document 13851/4/04 rev 4

Analysis of Member States' coordination structures reveals (i) a number of horizontal best practices to strengthen coordination among **all** Relevant Actors and (ii) areas where measures specific to **certain** Relevant Actors may enhance coordination and information exchange. The former is addressed in Section 1 while coordination issues specific to certain Relevant Actors are set out in Sections 2. Section 3 addresses issues relevant to coordination between Relevant Actors and the private sector. In all cases particular attention should be paid to data protection rules, including safeguards on the accuracy of information held in relevant databases.

1. HORIZONTAL COORDINATION STRUCTURES INVOLVING ALL RELEVANT ACTORS

Analysis of national coordination structures reveals a number of horizontal best practices to strengthen information sharing at national level among all Relevant Actors and from which the following can be deduced:

1.1. **To help address policy coordination, consideration may be given to establishing a national framework comprising all Relevant Actors.** This will help build consensus around a national CFT strategy. It should promote confidence building, understanding and trust between agencies. Core tasks should include production of a Joint Counter Terrorism Action Plan, joint CFT risk and threat analyses and other joint CFT research[11]. Structures should be put in place to ensure that Relevant Actors are consulted, contribute to and have to sign off joint analysis of intelligence on methods used by terrorists to finance their activities. The benefits of including appropriate private sector representatives in this work should also be considered.

1.2. **To help address operational issues, consideration may be given to bring together Relevant Actors from intelligence services, law enforcement, Prosecutors' Office, FIU, tax revenue services and financial regulators**. Such a group could have a mandate to review investigation files from a range of angles. Operational benefits could include: (i) revealing leads that may otherwise go undetected; (ii) recommending changes in the way investigations are carried out and ensure investigations are intelligence based; (iii) avoid duplication; (iv) help establish links between suspects (v) facilitate joint assessment of related investigations.

1.3. **Operational coordination could be further enhanced by national networks, connecting in each Member State the respective FIU with, on the one hand, reporting bodies and, on the other hand the Relevant Actors.** This would create an automated yet secure electronic environment for the receipt, processing and dissemination of financial intelligence. It would enable the direct transfer of information from financial institutions into special databases in the FIU, support the computer-assisted production of financial intelligence within the FIU and allow for the automated exchange of information between FIU and Relevant Actors. This work is currently being assessed in the FIU NET project.

[11] One Member State highlighted the value of joint analysis of regular thematic investigations such as underground financial movements connected with the financing of terrorism.

1.4. **Minimum standards for collection, analysis and dissemination of intelligence.** This would facilitate intelligence generation and sharing and promote an intelligence driven and risk based approach. Standards should emphasise the need to derive meaning and value from collected information and a common commitment to disseminate that information rapidly to authorised persons in other Relevant Actors.

1.5. **Developing minimum standards for handling information** such as confidentiality levels, security clearances, document handling codes would facilitate and expand rapid and effective information exchange among Relevant Actors.

1.6. **Financial intelligence should support and supplement overall counter terrorist activity.** Integration within general counter terrorist activity of input from a body responsible for CFT coordination would help ensure that financial intelligence is an integral part of counter terrorist activity. This should also produce value in bridging the gap that may exist between specialised CFT police, Counter Terrorist police and intelligence services.

2. COORDINATION STRUCTURES SPECIFIC TO CERTAIN RELEVANT ACTORS

2.1. A number of Member States said they **had formalised terrorist financing information exchange structures between the Finance, Interior and Justice Ministries** and described how this process had given a new impetus to the fight against terrorist financing by bringing together the intelligence services, specialised police and FIU.

2.2. Some Member States indicated the benefits of an **inter-departmental body dedicated to identification, tracing and freezing of criminal/terrorist assets.** Such "Asset Investigation Bodies" with highly developed financial investigation skills, should be able to draw on complementary skills of police, Prosecutors, Tax Revenue services, customs and other relevant services and provide a source of expertise for all terrorist (and other serious criminal) investigations.

2.3. Member States should **promote awareness among law enforcement of the role the FIU can play in assisting their fight against terrorism financing** and other criminality. The use of Memoranda of Understanding between the FIU and other agencies may help to provide the framework for efficient access to financial information.

2.4. CFT experts within the FIU should have **appropriate security clearance** to allow them to receive, transmit and jointly analyse financial intelligence with intelligence services or other Relevant Actors handling security coded data. The need for appropriate security clearances within other Relevant Actors should also be considered so that classified information can be shared and jointly analysed where necessary.

Enhance mutual understanding among Relevant Actors

2.5. Coordination in the fight against terrorist financing is likely to be facilitated where **the FIU includes a dedicated CFT unit** facilitating closer coordination with CFT and CT experts in other Relevant Actors. Focused CFT experts within the FIU also ensure a greater awareness of CFT typologies and so facilitate identification and prioritisation of high risk cases. These expert units should ensure a multi-agency approach through structured coordination with police, prosecutors and intelligence services. Such units should be encouraged to compare approaches with their counterparts in other Member States.

2.6. To enhance mutual understanding, particularly where no formal structures exist, Member States should encourage **secondment of investigative magistrates, prosecutors, financial investigators, analysts and others to the FIU** as well as to and from other Relevant Actors.

2.7. **Relevant Actors must clearly understand each other's roles and ensure that systems are in place to allow information to move quickly to those best placed to act on it.** This would ensure, for example, that police or judicial information on known suspects is rapidly transmitted to Foreign Ministry officials responsible for requesting designation by the Council or the UN Security Council so as to have preventive financial restrictive measures (sanctions) applied to their funds and assets. Investigating authorities should consider whether the requirements for administrative freezing measures are met and whether such freezing is opportune, and in appropriate cases, formulate request for application of such measures. Similarly where cash is seized, whether at the border by customs or elsewhere, and there is a suspicion that this may be associated with terrorism, the FIU should be informed to raise prospects of finding linked information.

Ensure optimal use of Financial Intelligence

2.8. **Use of key words, key names and other identifiers to encourage immediate identification of terrorist related suspicious transaction reports.** Appropriate forms of co-operation should be established between FIUs and operational specialised services, including the exchange of information on suspicious transactions for intelligence purposes and possible disruption of terrorist acts.

Combine skill sets

2.9. **The complexity of CFT work is such that know how and expertise must frequently be combined, for example, by** allowing experts with complementary skills to be seconded on an ad hoc basis for a given project, investigation or prosecution. One Member State illustrated this citing structures created which allow and facilitate a prosecutor with expertise in financial crime to act jointly with a prosecutor with an anti-terrorism background in connection with CFT cases.

Outreach to wider Public

2.10. As well as ensuring that employees of reporting bodies are informed of typologies and threats, Member States in conjunction with financial and other institutions should ensure that ***users*** **of financial services are informed about how they can assist both public and private sector efforts** to combat the financing of terrorism and other financial crime.

3. RELEVANT ACTORS AND THE PRIVATE SECTOR

In many cases it is not so much the financial information per se held by banks and others which is of vital importance to law enforcement efforts, but rather the *intelligence* which that information can provide. For this reason it is essential to ensure good coordination between Relevant Actors and financial institutions (and other money laundering reporting bodies) so that necessary information can be obtained easily and rapidly and with appropriate guidance from Relevant Actors.[12] **Public sector intelligence can be enhanced by financial institution input.** For example, in some Member States important lead information has been obtained where sensitive information, such as data on forged identity documents, has been shared with financial institutions to identify and locate suspects.

Access to Private Sector financial information

3.1. **Measures to allow competent authorities to know whether a person subject to investigation has or has had a bank account and to obtain particulars of accounts and banking operations according to Article 32 of the third Anti-Money Laundering ("AML") Directive[13].** Some Member States indicated in answer to the above-mentioned questionnaire benefits of a national register of bank accounts in ensuring rapid identification of suspect funds and accounts. Such "registers" may range from a single central (constantly updated) database to encrypted customer lists held and controlled by financial institutions. Financial Intelligence Unit ("FIU") access on the basis of a suspicious disclosure report, would reveal on a hit/no hit basis whether a suspected person has or has had a bank account with a specified institution. An alternative model would allow law enforcement services investigating suspicion of terrorist financing to ask the FIU to enquire from financial institutions whether the suspect holds or has held an account. The Commission will undertake further work in conjunction with Member States and the private sector to assess models to implement Article 32 of the above Directive.

---

12 As regards *international* cooperation between Relevant Actors, this should be in compliance with Article 28 of the third AML Directive and should enhance and not reduce exchange of intelligence between FIUs.

13 Article 32 of the third Anti-Money Laundering Directive says "Member States shall require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the financial intelligence unit, or from other authorities in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of the business relationship"

3.2. Intelligence indicates that terrorists have used well known money transmission businesses with branches in different Member States to make a series of small transfers destined to persons associated with extremist groups. Individually each of these transfers may appear legitimate. Looked at collectively they may raise suspicions. Money **transmission and remittance businesses should ensure they have systems allowing them** to comply with international standards on originator's information as well as with the risk based approach to AML/CFT measures, including appropriate monitoring of suspicions.

3.3. Good practice indicates that suspicious activity should be reported to the FIU **even where it does not relate to a transaction**, such as where strong enough suspicion surrounds a financial institution rejection of an application to open an account for example where the person fails to provide adequate identifying information.

Promoting Cooperation with Private Sector

3.4. Encourage effective operation of ***liaison committees*** **between one or more Relevant Actors and representatives of financial and credit institutions and other reporting bodies.** Regular meetings of liaison committees, chaired by the national CFT coordinating body and/or the FIU, are an essential means of mobilising and providing outreach to the private sector, informing it of developing typologies in terrorist financing and updating risk indicators. In addition to structured liaison committees, dedicated CFT contact points should exist in financial institutions to facilitate rapid contact by FIU and other Relevant Actors. Regular feedback to reporting bodies will help ensure high quality reports to FIUs.

3.5. Reporting bodies operating in more than one Member State should aim to ensure coordination among national compliance officers, for example through a **"Europe compliance function"**. This would seek both to establish links between suspicious transactions identified in two or more Member States and to establish or reinforce suspicions in the case of related transactions to or from two or more Member States.

3.6. **Secondment even for a short period, of financial police / FIU staff / intelligence personnel to private sector data holders should be encouraged.** This enhances public sector understanding of how private sector data are managed and the ease or difficulty involved in retrieving certain types of information.

PART II - VULNERABILITIES OF NPOS TO TERRORIST FINANCING AND OTHER CRIMINAL ABUSE

1. EUROPEAN AND INTERNATIONAL CONTEXT

The Commission's October 2004 Communication on terrorist financing raised the possibility of a Code of Conduct to reduce the risk of abuse of the non-profit sector[14]. The Recommendation and the Framework for a Code of Conduct presented in this document are therefore a follow-up to that Communication. While the focus of the present Communication is to prevent abuse of NPOs by terrorist financing, the enhanced transparency and

[14] COM(2004) 700 of 20.10.2004 see Section 5.2

accountability measures will also help to protect organisations from other forms of criminal abuse. The Recommendation and the Framework for a Code of Conduct should therefore enhance donor confidence, encourage more giving, while preventing or at least reducing the risk of criminal abuse.

Following the 9/11 terrorist attacks, the Financial Action Task Force ("FATF") adopted a series of "Special Recommendations" specific to terrorist financing. These included a Recommendation[15] that countries should address the vulnerabilities of the non-profit sector. In practice Member States and third countries have found it difficult to implement this element of the Special Recommendations. Significant discussions have taken place within the FATF on possible approaches. To date FATF members have been unable to agree a common approach to implementation of Special Recommendation VIII.

The importance of the area has also been acknowledged by EU Member State Governments and other international bodies[16]. The EU Joint Strategy Paper[17] on Terrorist Financing and the European Council Conclusions of 16-17 December 2004 asked the Commission to address the misuse of NPOs for terrorist financing purposes. The Council Declaration on the EU response to the London bombings of 13th July 2005 calls on the Council to "agree a Code of Conduct to prevent the misuse of charities by terrorists".

Taking account of the potential vulnerabilities of the non-profit sector to terrorist financing and other criminal abuse, the Commission addresses a Recommendation to Member States and a Framework for a Code of Conduct for NPOs acting in the European Union.

The Commission has extensively consulted with Member States and the non-profit sector during the preparation of the Recommendation and Framework for a Code of Conduct including an eight week internet-based public consultation.

2. IMPLEMENTATION AT THE EUROPEAN LEVEL

The Commission should assure ***further dialogue with the non-profit sector*** on the follow up to the Recommendation and Framework for a Code of Conduct presented in this Communication.

In particular, during the course of first half of 2006, the Commission will set up an ***informal contact group*** and organise a ***conference*** with representatives of the non-profit sector and relevant authorities to consider possible ways of further implementation of principles laid down in the Recommendation and Framework for a Code of Conduct.

---

15 Special Recommendation VIII states: « …Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused (i) by terrorist organisations posing as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing…and (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations."

16 The Financial Action Task Force in its Special Recommendation VIII; G8 Finance Ministers, "Finance Ministers' Statement" of Deauville, 17 May 2003; G8 Justice and Home Affairs Ministers, "Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks", Washington, 11 May 2004.

17 ibid

It should be further discussed with relevant stakeholders how partnership between NPOs and state authorities could be developed to find an ***appropriate balance between statutory and self-regulation for the non-profit sector***.

The European Commission will further consider whether ***in certain circumstances, Community funding of NPOs*** could be linked to compliance with enhanced transparency and accountability measures.

The Commission will ***assess the results achieved by the Recommendation and Framework for a Code of Conduct*** three years from its date of adoption.

ANNEX

Recommendation for Member States and a Framework for a Code of Conduct for NPOs to Enhance Transparency and Accountability in the Non-profit Sector to Prevent Terrorist Financing and other Types of Criminal Abuse

1. INTRODUCTION

The non-profit sector carries out vital humanitarian and other much needed public work, where citizens benefit from their indispensable services in fundamental areas of life. NPOs are essential parts of democratic societies that often fulfil crucial tasks that other types of organisations or public bodies cannot achieve.

However, there is evidence that in several instances NPOs have been exploited for the financing of terrorism and for other criminal ends[18] and, in some cases, administrative freezing measures[19] have been imposed to prevent such exploitation. Terrorists and terrorist organisations can access finance through different sources. Money can be transferred through the financial sector, through wire transfers, alternative remittance systems and via cash courriers, but funds can also be moved and raised under the cover of NPOs. The Financial Action Task Force stated in its Report on Money Laundering and Terrorist Financing Typologies 2003-2004 that *"The case examples presented during this year's typologies exercise appeared to show that NPOs can be misused in a variety of ways and for different purposes within the framework of terrorism financing. First of all, NPOs can be used by terrorists and terrorist organisations to raise funds, as was the case for many of the larger NPOs that had their assets frozen on the basis of the UN Security Council Resolution 1373 (2001)…. A number of the experts noted the importance of informal cash collection in many ethnic or religious communities and the difficulties in accurately monitoring those funds…. NPOs can also be used by terrorists to move funds…. Finally, NPOs can also be used to provide direct logistical support to terrorists or serve as a cover for their operations."* [20]

Higher and/or more systematic standards of transparency and accountability applied by NPOs will help to strengthen the non-profit sector against criminal abuse. The present document aims to find an approach that minimises this risk of abuse without over-burdening the sector. The basic principles set out in the Communication should in no way be interpreted so as to restrict the freedom of association. Particular attention should be paid to data protection rules. Moreover, implementation of the Recommendation to Member States and the Framework for a Code of Conduct should not jeopardise the efficient provision of emergency relief and other non-profit activity where needed. Care must be taken to ensure that nothing is done that could

---

[18] Experts of the FATF analysed cases of misuse of NPOs for terrorist financing for example in the *Report on Money Laundering and Terrorist Financing Typologies 2003-2004* available at http://www.fatf-gafi.org/dataoecd/19/11/33624379.PDF; other examples can be found at the homepage "Inquiry Reports" of the Charity Commission for England and Wales at http://www.charitycommission.gov.uk/investigations/inquiryreports/inqreps.asp

[19] The freezing measures are based on Regulation (EC) No 881/2002 of 27 May 2002 (OJ L 139, 29.5.2002, p.9) as amended, or on Regulation (EC) No 2580/2001 of 27 December 2001 (OJ L 344, 28.12.2001, p.70) as amended.

[20] See pages 8-10 in the *Report on Money Laundering and Terrorist Financing Typologies 2003-2004* at http://www.fatf-gafi.org/dataoecd/19/11/33624379.PDF

undermine the work or reputation of the vastest majority of NPOs legitimately operating at national, EU and international levels.

NPOs in the European Union are very heterogeneous in size and legal form[21]. For the purposes of the Recommendation to Member States and the Framework for a Code of Conduct, NPOs are deemed to be organisations, legal persons, legal arrangements whose principal purpose is to "engage in the raising and/or disbursing funds for charitable, religious[22], cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works."[23]. For reasons of diversity, it would be appropriate to avoid a "one-size-fits-all" approach[24]. Furthermore, the Recommendation and the Framework for a Code of Conduct should not in any way hinder legal cross border activities of NPOs. The aim of a European approach is thus to establish common principles on which national implementation can be based.

2. RECOMMENDATION TO MEMBER STATES TO ADDRESS THE VULNERABILITIES OF THE NON-PROFIT SECTOR TO TERRORIST FINANCING AND TO OTHER CRIMINAL ABUSE

The following Recommendation is addressed to Member States to help them to assess how far progress has been achieved in the fight against the misuse of NPOs for terrorist financing and other criminal purposes and to identify what further measures could be taken at the national level. Member States should encourage NPOs to apply enhanced transparency and accountability measures in their daily management in order to reduce the scope of their misuse for criminal purposes. Member States should ensure that their national non-profit sector is fully engaged in implementation at national level.

2.1. Oversight of the non-profit sector

– Member States should ensure that they have oversight of their non-profit sector. The oversight role could either be dedicated to a single public body or entrusted to existing authorities or to self-regulatory bodies.

– Bodies that have oversight of the non-profit sector, or a part of it, should ensure efficient national cooperation. In this role, they should:

---

21 The diversity of the sector has already been described by the Commission Communication "Promoting the role of voluntary organisations and foundations in Europe" COM(1997) 241.

22 Declaration 11 in the Annex to the Amsterdam Treaty states *"The European Union respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States. The European Union equally respects the status of philosophical and non-confessional organisations."*

23 Based on the definition given by the Financial Action Task Force Special Recommendation VIII Best Practices Paper.

24 To avoid such an approach, the registration of those NPOs is suggested that are wishing to take advantage of special tax treatment, access to public grants, the right to public fundraising; the Framework for a Code of Conduct emphasises the application of simplified accounting and reporting rules for NPOs under a certain size.

- Operate publicly accessible registration systems for all NPOs operating on their territory and wishing to take advantage of preferential tax treatment, the right to public fundraising and access to public sector grants. These registration systems might be operated at national, regional or municipal level. Special attention has to be given that the registration fully respects the principle of freedom of association. Thus, registration would take the form of a notice of constitution rather than a prior approval for constitution;

- identify existing requirements on NPOs to avoid duplication of registration/ reporting obligations;

- Identify any categories of NPOs that fall outside the limit of their registration systems and mitigate the risk that these gaps might pose;

- Provide guidance to NPOs on financial transparency and on vulnerabilities of the sector;

- There should be coordination among competent bodies with regard to investigation of abuse of NPOs. Investigation should follow existing criminal law procedures. Competent bodies should also have the capacity to assess risk of abuse of individual NPOs;

- Tax Authorities should be encouraged to carry out reviews of NPOs receiving special tax treatment, with due consideration of the size and activity of the organisation.

2.2. Encourage compliance with Code of Conduct

To promote compliance, Member States should consider the following issues:

– Registration, enhanced transparency and accountability standards ***confirm a visible status for NPOs*** and help to acquire and maintain public trust and credibility of non- profit work;

– ***Privileged Tax Status, the award of public grants and the right to public fundraising*** could be offered to all NPOs fulfilling the registration requirement and complying with transparency and accountability measures. A mechanism to ensure compliance may be a certification model as described below;

– It may be appropriate in the future to consider including the transparency and accountability principles proposed in the Framework for a Code of Conduct ***in existing labels or in labels to be developed***. Such systems could be run by public or private bodies and would examine compliance of NPOs with the transparency and accountability measures;

– ***Private monitoring bodies or non-profit umbrella organisations*** should be encouraged to establish seals of approval or other similar mechanisms for NPOs compliant with the principles of the Framework for a Code of Conduct.

2.3. Outreach and Vulnerabilities of NPOs to Terrorist Financing and other Criminal Purposes

Intelligence continues to indicate[25] that misuse of the non-profit sector remains to be one of the methods used by terrorists to raise funds to finance their activities. It is therefore of key importance that Member States and NPOs are fully aware of how organisations may be misused for terrorist financing and other criminal purposes.

- NPOs should be encouraged to **assess their existing good practices** to strengthen further the prevention of their misuse for terrorist financing and other criminal purposes;

- With the involvement of key actors of the non-profit sector, Member States should initiate **awareness programmes for NPOs** on risks/vulnerabilities of the sector to abuse;

- **Guidance should be provided for the private sector** (financial institutions, accountants, auditors and lawyers dealing with the non-profit sector) to facilitate detection of suspicious activity/transactions, including techniques notably used for infiltration of NPOs by terrorists.

2.4. Investigation of abuse of NPOs

The investigation should be proportionate to the weight of identified risk and follow existing criminal law procedures.

- Co-operation/information exchange ***at national level*** should be led and coordinated, if possible, by one of the competent authorities with responsibility for overseeing NPOs and include Tax Authorities, Financial Intelligence Unit, and law enforcement services. To facilitate national level information exchange, a person should be nominated in each of these entities representing the single point of contact for information exchange purposes in cases related to misuse of NPOs for terrorist financing. Dedicated information gateways should be established among these entities to ensure rapid and effective exchange.

- Co-operation/information exchange ***at EU/international level*** should comprise a network made up of law enforcement single contact points with expertise in terrorist financing and knowledge of the NPO sector. The Commission will promote the use of existing EU level co-operation/information exchange networks among law-enforcement authorities and, where appropriate, other bodies competent to investigate possible abuse of NPOs. The European Anti Fraud Office (OLAF) could fulfil a particular role in this co-operation and information exchange. The role of *CEPOL (European Police College)* could be crucial in training senior police officers in highlighting vulnerabilities of the sector, typologies of abuse, promoting cooperation/information exchange.

---

[25] See for example Europol's « Overview of the fight against financing of terrorism in the European Union » Restricted 1st June 2005

3. CONSIDERATIONS FOR THE NON-PROFIT SECTOR - FRAMEWORK FOR A CODE OF CONDUCT FOR NPOS TO PROMOTE TRANSPARENCY AND ACCOUNTABILITY BEST PRACTICES

In a non-profit sector where enhanced levels of transparency and accountability are applied, there is less possibility for criminal abuse to occur. A considerable part of NPOs already follows most of the requirements set out in this document and many have also created their own Codes of Conduct. By applying these rules, NPOs demonstrate their responsibility towards public generosity and strengthen themselves against criminal abuse. The principal aim of the requirements of this Framework for a Code of Conduct is thus to find common general minimum transparency standards for NPOs in the European Union and to promote further discussions in this area.

– The NPOs should pursue the ***mission purpose*** of the organisation and should use their resources for these purposes.

– Responsibility of legal compliance should lie with the ***highest governing body*** of the organisation.

– All NPOs should produce a ***document containing identification information*** on the organisation. This record should be kept up to date and available at the NPO's office. Registered NPOs should send this identification information to the body responsible for fulfilling relevant registration functions. This body should be informed of changes in the key features of the organisation and of winding-up of the organisation (together with a statement on how the net assets of the NPO will be distributed).

The information should clearly identify the NPO. In addition to the formal name of the NPO, additional information could include any commonly used acronym or other informal name, business/working name and registration number (if appropriate). It would further include information on the address of the registered office, telephone/fax number/web site address and a record of previous addresses and changes of address. Details of sub branches of the organisation would also be included. A statement of the General Objectives, Policies and Priorities (mission purpose) of the NPO should be further mentioned, including a description of the NPO's organisational and decision-making structure - reflecting the size of the organisation and indicating internal financial control systems. The document should identify directors/ executive committee members or other decision makers of the organisation and their responsibilities. Where appropriate the beneficial owner of the NPO would also be identified.

List of the bank account numbers under the name of the NPO and any data on personal details should be kept confidentially on the register and at the NPO's office.

– NPOs should follow ***proper book-keeping practice*** and produce ***annual financial statements*** of income and expenditure. A ***report*** should be prepared annually containing the description and budget of activities, projects over the previous financial year and include a statement of how these have promoted the NPO's General Objectives. In order to avoid overburdening NPOs with excessive administrative requirements, ***Simplified accounting and reporting requirements*** should apply to NPOs under a certain size[26].

[26] Member States might determine other criteria (e.g. areas of activity) for NPOs subject to simplified accounting and reporting requirements.

Financial statements and reports should be kept available at the office of the NPO accessible at request of public authorities having oversight responsibility.

– Annual financial statements and reports, minutes of meetings of decision making bodies, records on audit trails[27] should be ***held for at least 5 years*** at the registered office of the NPO.

– NPOs should use ***formal channels*** for money flows for all transactions, whenever there is a reasonable possibility to use the formal financial system. To the extent practicable, all money received should be deposited in bank accounts and the disbursement of money should be performed by means of these bank accounts.

– All NPOs should follow the ***"Know your beneficiaries and associate NPOs"*** rule, which means that the NPO should make best endeavours to verify the identity, credentials and good faith of their beneficiaries and associate NPOs. This could include for example, in advance of payment, the NPO determining that the potential recipient has the ability both to accomplish the charitable purpose of the grant and protect the resources from diversion to non-charitable purposes. Where practicable, the NPO should reduce the terms of the grant to a written agreement and engage in on-going monitoring.

– NPOs should keep full and accurate ***audit trails of funds*** transferred outside their jurisdiction/ country and of funds transferred to any person delivering service on behalf of the originator NPO. This could include keeping appropriate records of all financial transactions to direct intermediary organisations and persons.

[27] As described at point addressing requirements on *audit trails of funds*.