



**EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS  
PRINCIPLES FOR INFORMATION EXCHANGE BETWEEN  
FINANCIAL INTELLIGENCE UNITS**

Approved by the Egmont Group Heads of Financial Intelligence Units

July 2013

## Table of contents

A. Introduction .....	3
B. General framework .....	3
C. International Co-operation .....	4
<b>Obligations for the FIU making the request</b> .....	4
<b>Obligations for the FIU receiving the request</b> .....	5
<b>Unreasonable or unduly restrictive conditions and cases for refusal to international co-operation</b> .....	5
<b>Data protection and confidentiality</b> .....	6
<b>Channels for the exchange of information</b> .....	6



## EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS PRINCIPLES FOR INFORMATION EXCHANGE BETWEEN FINANCIAL INTELLIGENCE UNITS

These Principles are binding. Therefore, cases of significant and relevant non-compliance will be subject to the *Egmont Group Support and Compliance Process*.

### A. Introduction

1. The Egmont Group fosters the development of Financial Intelligence Units (FIUs) and information exchange.
2. The Egmont Group agreed in its Charter and Statement of Purpose to pursue among its priorities the stimulation of information exchange and to overcome the obstacles preventing cross-border information sharing.
3. The Egmont Group membership affirms accession to the standards set out in the 2012 revised Financial Action Task Force (FATF) Recommendations and Interpretative Notes on Financial Intelligence Units (*Recommendation 29*) and Other Forms of International Co-operation (*Recommendation 40*).
4. The definition of a Financial Intelligence Unit (FIU) is as stated within the Charter.
5. Information-sharing arrangements should aim to foster the widest possible co-operation between FIUs.
6. The following principles outline generally shared concepts, while allowing necessary flexibility.

### B. General framework

7. International co-operation between FIUs should be encouraged and based upon a foundation of mutual trust.
8. Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.

## C. International Co-operation

9. FIUs should exchange information with foreign FIUs, regardless of their status; be it administrative, law enforcement, judicial or other.
10. To this end, FIUs should have an adequate legal basis for providing co-operation on money laundering, associated predicate offences and the financing of terrorism.
11. FIUs should exchange information freely, spontaneously and upon request, on the basis of reciprocity. FIUs should ensure that they can rapidly, constructively and effectively provide the widest range of international co-operation to counter money laundering, associated predicate offences and the financing of terrorism. FIUs should do so both spontaneously and upon request, and there should be a lawful basis for providing co-operation.
12. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly.
13. In order to conduct proper analysis, FIUs should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.
14. FIUs should be able to disseminate, spontaneously and upon request, information and the results of their analysis to relevant competent authorities.
15. FIUs should use the most efficient means to co-operate. If bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), are needed, these should be negotiated and signed in a timely way with the widest range of foreign FIUs in the context of international co-operation to counter money laundering, associated predicate offences and terrorist financing.
16. FIUs should be able to conduct queries on behalf of foreign FIUs, and exchange with these foreign FIUs all information that they would be able to obtain if such queries were carried out domestically.

### **Obligations for the FIU making the request**

17. When requesting co-operation, FIUs should make their best efforts to provide complete, factual and, as appropriate, legal information including the description of the case being analyzed and the potential link with the country receiving the request. This includes indicating any need for urgency, to enable timely and efficient execution of the requests.
18. FIUs may decide to exchange information indirectly with non-counterparts in response to requests from competent authorities. FIUs should ensure that the competent authority requesting the information indirectly always makes it clear who they are requesting the information for, and for what purpose.

19. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.
20. An FIU requesting information should disclose, to the FIU that will process the request, the reason for the request, and to the extent possible the purpose for which the information will be used, and provide enough information to enable the FIU receiving the request to provide information lawfully.
21. Requests for information that are sent simultaneously to several FIUs should be justified with a clear explanation of the link that involves the specific set of countries. Requests for information should not be sent to large distribution lists if the link is not justifiable to all recipients.

#### **Obligations for the FIU receiving the request**

22. FIUs should have the power to exchange:
  - a. All information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and
  - b. Any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.
23. FIUs should acknowledge receipt of requests, respond to requests for information, and provide interim partial or negative responses in a timely manner.

#### **Unreasonable or unduly restrictive conditions and cases for refusal to international co-operation**

24. FIUs should not prohibit or place unreasonable or unduly restrictive conditions on exchanging information or providing assistance. In particular, FIUs should not refuse a request for assistance on the grounds that:
  - a. The request is also considered to involve fiscal matters;
  - b. Laws require financial institutions or designated non-financial businesses and professions (except where the relevant information that is sought is held under circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality;
  - c. There is an inquiry, investigation or proceeding underway in the country receiving the request, unless the assistance would impede that inquiry, investigation or proceeding; and/or
  - d. The nature or status (civil, administrative, law enforcement etc.) of the requesting counterpart authority is different to its foreign FIU.
25. FIUs receiving requests may, as appropriate, refuse to provide information if the requesting FIU cannot protect the information effectively.
26. FIUs receiving requests should promptly, and to the largest extent possible, grant prior consent to disseminate the information to competent authorities. The FIU receiving the request should not

refuse consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could impair a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the State of the providing FIU, or would otherwise not be in accordance with fundamental principles of its national law. Any such refusal to grant consent should be appropriately explained.

27. Co-operation may also be refused, as appropriate, on the grounds of lack of reciprocity or recurring inadequate co-operation. All cases that are refused must be justified, and FIUs should make all efforts to provide an explanation when the requested co-operation cannot be provided.

#### **Data protection and confidentiality**

28. Information received, processed, held or disseminated by requesting FIUs must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations.
29. FIUs must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination and protection of, as well as access to, such information.
30. FIUs should ensure their staff members have the necessary security clearance levels and understand their responsibilities in handling and disseminating sensitive and confidential information.
31. FIUs should ensure there is limited access to their facilities and information, including information technology systems.
32. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorization by the requested FIU.
33. At a minimum, exchanged information must be treated and protected by the same confidentiality provisions that apply to similar information from domestic sources obtained by the FIU receiving the request.

#### **Channels for the exchange of information**

34. Exchanges of information should take place in a secure way, and through reliable channels or mechanisms.
35. To this end, FIUs should use the Egmont Secure Web or other recognized networks that ensure levels of security, reliability and effectiveness at least equivalent to those of the Egmont Secure Web (for example, the FIU.NET).
36. FIUs should ensure access to, and use of, the Egmont Secure Web or other appropriate channels of communication are securely protected and reserved to authorized personnel. The equipment and passwords used for these channels should also be securely protected.
37. FIUs should be aware of the standards of security, reliability, efficiency and effectiveness applied in the use of the Egmont Secure Web or other appropriate channels.