



GENERAL FISHERIES COMMISSION
FOR THE MEDITERRANEAN
COMMISSION GÉNÉRALE DES PÊCHES
POUR LA MÉDITERRANÉE



GENERAL FISHERIES COMMISSION FOR THE MEDITERRANEAN

Second session of the Compliance Committee

Rome, Italy, 25-26 February 2008

**RECOMMENDATION GFCM/2006/7 ON DATA CONFIDENTIALITY
POLICY AND PROCEDURES**

The General Fisheries Commission for the Mediterranean (GFCM),

RECOGNISING the need for confidentiality at the commercial and organisational levels for data, reports and messages submitted to GFCM, the following policy and procedures on confidentiality of data will apply;

ADOPTS, in accordance with paragraph 1 (h) of Article III and with Article V of the GFCM Agreement that:

1. Field of application

The provisions set out below shall apply to all data, reports and messages (electronic and of other nature) transmitted and received pursuant to GFCM recommendations

2. General Provisions

- a) The Executive Secretary and the appropriate authorities of the Contracting Parties and Cooperating Non-Contracting Parties, transmitting and receiving data, reports and messages shall take all necessary measures to comply with the security and confidentiality provisions set out in sections 3 and 4.
- b) The Executive Secretary shall inform all Contracting Parties and Cooperating non-Contracting Parties of the measures taken in the secretariat to comply with these security and confidentiality provisions.

- c) The Executive Secretary shall take all the necessary steps to ensure that the requirements pertaining to the deletion of data, reports and messages handled by the Secretariat are complied with.
- d) Each Contracting Party and Cooperating non-Contracting Party shall guarantee the Executive Secretary the right to obtain as appropriate, the rectification of data, reports and messages the processing of which does not comply with the provisions of the GFCM Agreement.
- e) The Commission may instruct the Executive Secretary not to make available the data, reports and messages received by a Contracting Party and Cooperating non-Contracting Party, where it is established that the Contracting Party and Cooperating non-Contracting Party in question has not complied with these security and confidentiality provisions.

3. Provisions on Confidentiality

Data, reports and messages shall be used only for purposes stipulated in GFCM recommendations.

4. Provisions on Security

- a) Contracting Parties and Cooperating Non-Contracting Parties and the Executive Secretary shall ensure the secure treatments of data, reports and messages, in particular where the processing involves transmission over an electronic network. Contracting Parties and Cooperating Non-Contracting Parties and the Executive Secretary must implement appropriate technical and organisational measures to protect data, reports and messages against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all inappropriate forms of processing.

The following security issues must be addressed from the outset:

- System access control: the system has to withstand a break-in attempt from unauthorised persons.
- Authenticity and data access control: the system has to be able to limit the access of authorised parties to a predefined set of data only.
- Communication security: it shall be guaranteed that data, reports and messages that enter the system are securely communicated.
- Data security: it shall be guaranteed that data, reports and messages that enter the system are securely stored for the required time and that they will not be tampered with.
- Security procedures: security procedures shall be designed addressing access to the system, system administration and maintenance, backup and general use of the system.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing of the data, reports and messages.

b) Data Security

Access limitation to the data shall be secured via a flexible user identification and password mechanism. Each user shall be given access only to the data necessary for his task.

c) Security Procedures

Each Contracting Party and Cooperating Non-Contracting Party and the Executive Secretary shall nominate a security system administrator. The security system administrator shall review the log files generated by the software, properly maintain the system security, restrict access to the system as deemed needed and act as a liaison with the Executive Secretary in order to solve security matters.