Annex X

INTERNATIONAL ORGANIZATION FOR MIGRATION

IOM DATA PROTECTION PRINCIPLES

1. LAWFUL AND FAIR COLLECTION

Personal data must be obtained by lawful and fair means with the knowledge or consent of the data subject.

2. SPECIFIED AND LEGITIMATE PURPOSE

The purpose(s) for which personal data are collected and processed should be specified and legitimate, and should be known to the data subject at the time of collection. Personal data should only be used for the specified purpose(s), unless the data subject consents to further use or if such use is compatible with the original specified purpose(s).

3. DATA QUALITY

Personal data sought and obtained should be adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. Data controllers should take all reasonable steps to ensure that personal data are accurate and up to date.

4. CONSENT

Consent must be obtained at the time of collection or as soon as it is reasonably practical thereafter, and the condition and legal capacity of certain vulnerable groups and individuals should always be taken into account. If exceptional circumstances hinder the achievement of consent, the data controller should, at a minimum, ensure that the data subject has sufficient knowledge to understand and appreciate the specified purpose(s) for which personal data are collected and processed.

5. TRANSFER TO THIRD PARTIES

Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data and to ensure that the rights and interests of the data subject are respected. These three conditions of transfer should be guaranteed in writing.

6. CONFIDENTIALITY

Confidentiality of personal data must be respected and applied to all the stages of data collection and data processing, and should be guaranteed in writing. All IOM staff and individuals representing third parties who are authorized to access and process personal data, are bound to confidentiality.

7. ACCESS AND TRANSPARENCY

Data subjects should be given an opportunity to verify their personal data, and should be provided with access insofar as it does not frustrate the specified purpose(s) for which personal data are collected and processed. Data controllers should ensure a general policy of openness towards the data subject about developments, practices and policies with respect to personal data.

8. DATA SECURITY

Personal data must be kept secure, both technically and organizationally, and should be protected by reasonable and appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer. The safeguard measures outlined in relevant IOM policies and guidelines shall apply to the collection and processing of personal data.

9. RETENTION OF PERSONAL DATA

Personal data should be kept for as long as is necessary, and should be destroyed or rendered anonymous as soon as the specified purpose(s) of data collection and data processing have been fulfilled. It may however, be retained for an additional specified period, if required for the benefit of the data subject.

10. APPLICATION OF THE PRINCIPLES

These principles shall apply to both electronic and paper records of personal data, and may be supplemented by additional measures of protection, depending inter alia on the sensitivity of the personal data. These principles shall not apply to non-personal data.

11. OWNERSHIP OF PERSONAL DATA

IOM shall assume ownership of personal data collected directly from data subjects or collected on behalf of IOM, unless otherwise agreed, in writing, with a third party.

12. OVERSIGHT, COMPLIANCE AND INTERNAL REMEDIES

An independent body should be appointed to oversee implementation of these principles and to investigate any complaints, and designated data protection focal points should assist with monitoring and training. Measures will be taken to remedy unlawful data collection and data processing, as well as breach of the rights and interests of the data subject.

13. EXCEPTIONS

Any intent to derogate from these principles should first be referred to the IOM Legal Affairs Department for approval, as well as the relevant unit/department at IOM Headquarters.

GLOSSARY

Anonymous data means that all the personal identifiable factors have been removed from data sets in such a way that there is no reasonable likelihood that the data subject could be identified or traced.

Consent means any free, voluntary and informed decision that is expressed or implied and which is given for a specified purpose.

Child means any person under the age of 18 years.

Data controller means IOM staff or an individual that represents a third party who has the authority to decide about the contents and use of personal data.

Data processing means the manner in which personal data is collected, registered, stored, filed, retrieved, used, disseminated, communicated, transferred and destroyed.

Data protection means the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data.

Data protection focal point means any IOM staff that is appointed by IOM Regional Representatives to serve as a contact or reference person for data protection and who is responsible for monitoring the data protection practices in the region to which they are assigned.

Data subject means an IOM beneficiary that can be identified directly or indirectly by reference to a specific factor or factors. These factors include a name, an identification number, material circumstances and physical, mental, cultural, economic or social characteristics that can be used to identify an IOM beneficiary.

Electronic record means any electronic data filing system that records personal data.

Inter alia (Latin) means "amongst other things."

IOM means the International Organization for Migration.

IOM beneficiary means any person that receives assistance or benefits from an IOM project.

IOM headquarters means IOM offices in Geneva, Switzerland.

IOM staff means all persons who are employed by IOM, whether temporarily or permanently, including formal and informal interpreters, data-entry clerks, interns, researchers, designated counselors and medical practitioners.

IOM unit/department means the structure at IOM headquarters responsible for IOM activity areas.

Knowledge means the ability to fully understand and appreciate the specified purpose for which personal data are collected and processed.

Non-personal data means any information that does not relate to an identified or identifiable data subject.

Paper record means any printed or written document that records personal data.

Personal data means any information relating to an identified or identifiable data subject that is recorded by electronic means or on paper.

Third party means any natural or legal person, government or any other entity that is not party to the original specified purpose(s) for which personal data are collected and processed. The third party that agrees in writing to the transfer conditions outlined in principle 5, shall be authorized to access and process personal data.

Vulnerable groups means any group or sector of society, including children, that are at exceptional risk of being subjected to discriminatory practices, violence, natural disasters, or economic hardships.

Vulnerable individual means any IOM beneficiary that may lack the legal, social, physical or mental capacity to provide consent.