

IOM DATA PROTECTION MANUAL



International Organization for Migration

IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM acts with its partners in the international community to: assist in meeting the operational challenges of migration; advance understanding of migration issues; encourage social and economic development through migration; and uphold the human dignity and well-being of migrants.

Publishers: International Organization for Migration
17 route des Morillons
1211 Geneva 19
Switzerland
Tel: +41.22.717 91 11
Fax: +41.22.798 61 50
E-mail: hq@iom.int
Internet: <http://www.iom.int>

© 2010 International Organization for Migration (IOM)

Cover illustration: © Yvonne Lee-www.allegoric.co.uk

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher.



IOM DATA PROTECTION MANUAL



IOM International Organization for Migration

FOREWORD

Data protection is an area of law that is constantly evolving. This is due to privacy concerns associated with the rapid growth of information technology and the fact that data are digitally transferable and easily accessible. The increased incidences of data theft, data loss, and unauthorized or inappropriate use and disclosure of personal data have resulted in questions relating to the effective implementation of laws and policies. In addition, the use of advanced technology in migration management and document fraud presents diverse challenges linked to data protection and human rights. These concerns are compounded in situations where inadvertent disclosure could result in harm or threat to the safety of individuals. Regardless of regular or irregular movements, when individuals reveal their personal data for a particular purpose, it should be handled with due care to protect their best interests and to ensure that they are fully aware of any implication on their human rights.

The international standards for collecting and processing personal data are acknowledged worldwide. However, the lack of a binding international instrument has been the subject of much debate. At the 31st International Conference of Data Protection and Privacy Commissioners, a resolution was adopted by a number of States calling for a universal convention and recognizing that data protection and privacy are fundamental rights attributed to all individuals, irrespective of nationality or residence. It is IOM's hope that content of this publication will add to the discussion of stakeholders, both nationally and internationally.

Notwithstanding the vast literature on this issue, there is limited guidance on protecting personal data in the context of migration. IOM is pleased to make an early contribution to the ongoing discussions on data protection and we encourage further engagement on this important issue. By way of background, IOM conducted a survey of selected registration projects in 26 field offices in 2007. The survey illustrated that there was indeed a need to standardize the handling of personal data throughout the Organization. IOM's policy on data protection is informed by relevant international standards, in particular the core data protection principles as recognized by many States, and through research on policies and procedures in other organizations. The IOM data protection principles are designed to assist IOM staff to take reasonable and necessary precautions in order to preserve the confidentiality of personal data and to ensure that the rights and interests of IOM beneficiaries are adequately protected. IOM's policy on data protection has been in force since May 2009 and lessons are learned on a daily basis. Although the content of this publication was developed for IOM use, it can be used as a resource tool by other organizations operating in similar contexts.

As a final point, acknowledgement is due to the author, Ruzayda Martens, for developing IOM's strategy on this issue and for advancing data protection as a necessary consideration in IOM's work.

ACKNOWLEDGEMENTS

The author would like to thank current and former IOM colleagues who pioneered the Technology Application and Migration Management (TAMM) Data Protection Project, a joint effort between the Department of Migration Management, the Department of Information Technology and Communications, and the International Migration Law and Legal Affairs Department. The Project benefited from the experience and expertise of a wide range of IOM colleagues, both in the Field and at Headquarters. Sincere thanks and appreciation are due to the Project Team, Steering Committee and Working Group members who took time out of their busy schedules to contribute at various stages of the project.

Firstly, particular thanks to the Project Team members: Shpëtim Spahiya for his contribution and support in the timely completion of the project and to Chiara Frattini, Jacqueline Straccia and Elif Celik for their research assistance.

Secondly, much appreciation to the Steering Committee members: Yorio Tanimura, Jillyanne Redpath-Cross and Bernardo Mariano for their expert guidance and indispensable contributions.

Thirdly, special thanks to the Working Group members for their commitment and detailed feedback: Nicholas Theotocatos, Norbert Wöhler, Monica Halil, Walter Brill, Sarah Craggs, Delbert Field, Lea Matherson, Jobste Koheler, Christopher Gascon, Elizabeth Dunlap, Dyane Epstein, Goran Grujovic, Chintana Meegamarachchi, Mariko Tomiyama, Teresa Zakaria and Jesus Sarol. Valuable comments were also received from various missions and individual colleagues; thanks are due to, amongst others: Jonathan Martens, Miwa Takahashi, Ashraf El-Nour, Richard Scott, Mio Sato, Amy Mahoney, Daniel Redondo, Ricardo Cordero, Tanja Brombacher, Mark Brown, Nasim Faruk, William Barriga, Gloria Ko, Patrick Corcoran, Abye Makonnen, Ramiro Nochez-McNutt, Anna Eva Randicetti, and Robert Villamor.

Finally, I wish to express my gratitude to Richard Perruchoud for his continuous support and to my colleagues at the Office of Legal Affairs for their efforts to promote data protection in their daily work.

Ruzayda Martens¹

¹ Legal Officer, IOM Geneva. It should be noted that the Data Protection Guidelines were developed to assist in the application of the 13 IOM data protection principles. The views, findings, interpretations and conclusions expressed in the Data Protection Guidelines are those of the author and the responsibility for any error remains that of the author.

TABLE OF CONTENTS		PAGE
	Introduction	9
PART I	IOM Data Protection Principles	11
PART II	Data Protection Guidelines	13
	How to use the guidelines	13
	Terminology	13
	Data protection	13
	Data subjects	14
	Personal data	14
	Data processing	15
	Risk–benefit assessment	16
	Data controllers	18
	Guiding points on IOM principles	
	Principle 1: Lawful and fair collection	19
	Principle 2: Specified and legitimate purpose	25
	Principle 3: Data quality	33
	Principle 4: Consent	39
	Principle 5: Transfer to third parties	49
	Principle 6: Confidentiality	57
	Principle 7: Access and transparency	63
	Principle 8: Data security	69
	Principle 9: Retention of personal data	79
	Principle 10: Application of the principles	85
	Principle 11: Ownership of personal data	91
	Principle 12: Oversight, compliance and internal remedies	95
	Principle 13: Exceptions	101
	Consideration boxes	
	1. Ethical considerations	15. Indicators for written transfer contract
	2. List of personal data	16. Confidentiality indicators
	3. Sensitivity assessment	17. Complaint considerations
	4. Risk action indicators	18. Access considerations
	5. Effective risk–benefit assessment	19. “Culture of data security” indicators
	6. Legal considerations	20. Consideration for electronic records
	7. Fairness considerations	21. Retention period
	8. Compatibility considerations	22. Further retention considerations
	9. Research considerations	23. Destruction considerations
	10. Reasonable steps to ensure accuracy	24. Depersonalizing personal data
	11. Assessing continued relevance	25. Ownership considerations
	12. Consent considerations	26. Compliance and oversight considerations
	13. Respecting vulnerability	27. Derogation considerations
	14. Foreseeable third parties	
	Annexure A: List of international instruments	105
	Annexure B: List of national legislation	107
	Glossary	109
	Bibliography	115
PART III	IOM Generic Templates and Checklists	127



INTRODUCTION

The collection and processing of personal data are necessary components of IOM's commitment to facilitate migration movements, understand migration challenges, and respect the human dignity and well-being of migrants. IOM's data protection strategy seeks to protect the interests of IOM beneficiaries, as well as the Organization itself.

Data protection is paramount for the safe exchange, secure storage and confidential treatment of personal data. To enhance IOM operations and systems, data protection should be applied systematically throughout the Organization.

IOM data protection statement

“IOM shall take all reasonable and necessary precautions to preserve the confidentiality of personal data and the anonymity of data subjects. All personal data shall be collected, used, transferred and stored securely in accordance with the IOM data protection principles.”

Key objectives:

- ✓ To respect privacy and meet the expectations of data subjects.
- ✓ To protect the integrity and confidentiality of personal data.
- ✓ To prevent unnecessary and inappropriate disclosure of personal data.
- ✓ To provide comprehensive institutional safeguards for the handling of personal data.
- ✓ To enhance understanding of core concepts and international data protection standards.
- ✓ To give operational guidance for the implementation of the IOM data principles and guidelines.

This publication provides practical guidance for protecting personal data in the context of migrant assistance. It consists of three parts: Part I outlines the 13 IOM data protection principles; Part II provides comprehensive data protection guidelines structured according to the 13 principles; and Part III consists of IOM operational templates and checklists.

- This publication is designed to be a living document. It is capable of adaption and revision to address emerging operational needs, policy developments and IOM systems upgrade or improvement.
- The application of the data protection measures outlined in this document may require a flexible approach, depending on the prevailing circumstances relating to project implementation.

The Office of Legal Affairs (LEG) at IOM Headquarters is the focal point on data protection issues and can assist with training to raise awareness among IOM staff and stakeholders.

PART I: IOM Data Protection Principles

IOM International Organization for Migration



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.

11

6. CONFIDENTIALITY

Confidentiality of personal data must be respected and applied at all 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 by 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 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 the 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 Office of Legal Affairs for approval, as well as the relevant unit/department at IOM Headquarters.

PART II: Data Protection Guidelines

The purpose of these guidelines is to govern the implementation of the IOM data protection principles (“IOM principles”) in a manner that recognizes both the right of individuals to protect their personal data and the need of IOM to collect, use and disclose personal data in the course of fulfilling its migration mandate.

Due to the multifaceted nature of IOM activities, data protection issues need to be considered at all stages, from project development and implementation to evaluation and reporting.

1. How to use the guidelines

The Data Protection Guidelines should be used in conjunction with other relevant IOM policies and guidelines and should be read as a “how to” tool for incorporating data protection into current practices of collection, storage, use, disclosure and disposal of personal data.

Consideration boxes are included and operational templates and checklists are available as practical tools to assist data controllers in identifying the key factors to be taken into account at the various stages of data processing.

Box 1: Ethical considerations

- ✓ Respect the privacy and dignity of data subjects.
- ✓ Ensure safety and non-discrimination.
- ✓ Protect confidentiality of personal data.
- ✓ Prevent unauthorized disclosure and inappropriate use of personal data.

2. Terminology



What is data protection?

Data protection is 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.²

All individuals have a right to privacy.³ The right to privacy is a universal right that is not restricted to nationals of a country, nor is there a distinction between non-nationals in a regular or an irregular situation. In its commitment to respect the human dignity and well-being of migrants and other beneficiaries, IOM seeks to ensure that personal data are handled with the utmost care and confidentiality. Improper use and unauthorized disclosure of personal data could result in a multitude of risks, ranging from physical violence to discrimination and social marginalization. A standardized approach to data protection throughout IOM will assist with effective management strategies to protect IOM beneficiaries, as well as the Organization itself. The IOM principles provide a framework for data protection and govern the handling of all types of personal data relating to IOM beneficiaries.

² The definition of data protection has been adapted for IOM purposes and draws a distinction between data protection and data security (see Glossary).

³ The IOM principles are based on relevant international instruments and standards. See Annexure A, which outlines the international and regional instruments governing the right to privacy and data protection, as well as Annexure B, which outlines national data protection legislation.



What about personal data relating to IOM staff?

Although the focus of the IOM principles are IOM beneficiaries; these principles create a benchmark for data protection throughout the Organization.



Who are data subjects?

Data subjects are individuals who can be directly or indirectly identified by reference to a specific factor or factors. Such factors may include a name, an identification number, material circumstances, and physical, mental, cultural, economic or social characteristics.

All identified or identifiable beneficiaries who fall within the scope of IOM activities are considered to be data subjects.



What is personal data?

Personal data include all information that could be used to identify or harm data subjects.

When handling personal data, data controllers should always consider sophisticated methods that could be used to identify data subjects.



What are sophisticated methods?

Sophisticated methods refer to extraordinary means of gaining unauthorized access to personal data, and require disproportionate time, effort, resource and determination.

Box 2 : List of personal data

- ✓ **Biographical data** such as name, date of birth, marital status, address or last place of residence, employment, contact details, age, language, sex, gender, sexual orientation, race, ethnic or social origin, nationality, religion, culture, political opinions or other beliefs, membership of a particular group, physical or mental disability and health status;
- ✓ **Biometric and genetic data** such as fingerprints, iris scans, hand patterns, facial image, voice recognition, and DNA samples;
- ✓ **Background data** such as family and household history, relationships with relatives, community members, and close associates;
- ✓ **Material circumstances** such as experience of human rights violations and transit details including route taken, education, employment history, work address, as well as names and contact details of IOM staff or individuals representing authorized third parties that conduct interviews and collect personal data;
- ✓ **Images and recordings** such as pictures or photographs, television images, videos, voice and digital recordings, medical X-rays, ultrasound and other medical images;
- ✓ **Corroborating materials** such as medical reports, psychological reports, hotline reports, police or other official and unofficial reports;
- ✓ **Personal documents** such as health records, financial records, bank details, and criminal records or activities;
- ✓ **Verification documents** such as originals or copies of passports, identity cards, social security cards, birth certificates, temporary permits, driver's licence, visas, marriage certificates, school diplomas, university records, medical certificates, property titles, and employment contracts or recruitment offers.

Note: This list is not exhaustive; it merely illustrates the types of personal data collected and processed in the context of IOM activities.

Sophisticated methods will vary depending on the sensitivity of the personal data and the nature of the IOM activity. Personal data that could be used to threaten the life of data subjects and IOM staff or individuals representing authorized third parties should be treated as highly sensitive.



EXAMPLE:

Links to organized crime may allow for highly organized tracking methods that could be used to identify and locate trafficked persons.



Data controllers should conduct a sensitivity assessment prior to data collection, in order to identify necessary safeguards, access controls and security measures to be applied throughout the life cycle of data processing.

The degree of sensitivity applied to personal data depends on the nature of the IOM project, type of IOM activity and the circumstances surrounding data collection and data processing. This includes, inter alia:

- the country situation;
- the target population group or individual data subject;
- social and cultural attitudes;
- potential physical harm; and
- discrimination that could result from disclosure.

Box 3: Sensitivity assessment

- High sensitivity;
- Moderate sensitivity;
- Low sensitivity.

Key considerations

- Potential to harm the data subject;
- Potential to discriminate;
- Potential to harm other data subjects;
- Potential to harm IOM staff and individuals representing authorized third parties.



It is important to highlight the level of sensitivity applied to electronic and paper records.

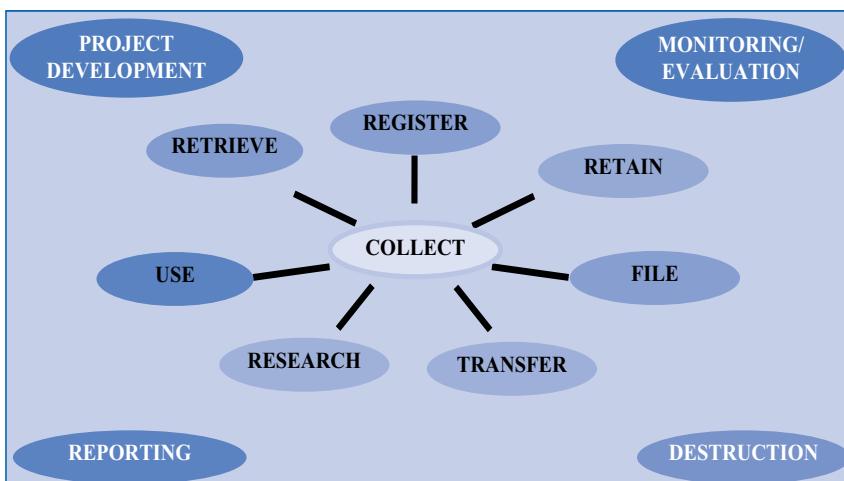


What is data processing?

Data processing is an overarching term that is used to describe all activities associated with the handling of personal data.

The IOM principles apply equally to all phases of data processing.

Diagram outlining the different phases of data processing



Note: Data processing is not necessarily a continuum from data collection to destruction, but often a range of activities that occur in parallel at various stages.

Data controllers should ensure that donors, IOM partners, implementing partners and other third parties are aware of IOM's commitment to safeguard personal data. This will foster cooperation and support the implementation of the IOM principles. Data controllers should incorporate the IOM principles into project proposals to cater for funding needs associated with, inter alia:

- data security measures;
- hardware and/or software devices;
- staff capacity; and
- training sessions.

The importance of training cannot be overemphasized. Training should focus on IOM staff and authorized third parties, as well as donors, IOM partners and implementing partners and other relevant stakeholders (see also principle 12).

What is a risk–benefit assessment?



Risk–benefit assessment is the process of evaluating the risks and benefits associated with data processing.

A risk–benefit assessment⁴ should be conducted prior to data collection and should apply to the substance, as well as the method of data collection and the means by which personal data will be captured, stored and subsequently used.



Data controllers should always weigh the probability of harm against the anticipated benefits, and ensure that the benefits significantly outweigh the potential risks.

Risks are dependent on the likelihood of it occurring and the severity of the harmful outcome. Even when unavoidable, risks can be reduced or managed. Precautions, safeguards, and feasible alternatives should be incorporated into project development strategies, as well as the data collection process, to reduce the possibility of harm or limit its severity or duration.



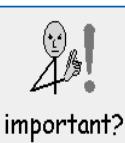
What happens if the risks outweigh the benefits?

Appropriate risk control measures should be implemented to prevent or mitigate the likelihood of the risk occurring. If the risk is too high, data controllers should discontinue the data processing.

Box 4 : Risk action indicators

- High risk: Unacceptable;
 - Moderate risk: Careful attention;
 - Low risk: Proceed with activity.
-
- High risk ➔ Immediately abandon the activity until measures to reduce the risk are implemented.
 - Moderate risk ➔ Apply careful attention and continuous monitoring, and, if necessary, stop the activity to implement measures to reduce the risk.
 - Low risk ➔ Proceed with the activity and continuously monitor the risk–benefit ratio.

⁴ The risk–benefit assessment is not a technical evaluation that is valid under all circumstances. Rather, it is a value judgement that often depends on various factors, including, inter alia, the prevailing social, cultural and religious attitudes of the target population group or individual data subject.



It is important to continually assess the risks and benefits throughout the life cycle of data processing because the risk–benefit ratio may change over time.

Risk control measures may include:

- ✓ **Elimination:** removing the risk is the safest and best way to reduce the risk.
- ✓ **Substitution:** substituting the hazard with something less risky is the best alternative if elimination is impossible.
- ✓ **Containment:** using strict supervisory controls can help minimize the likelihood of harm occurring.
- ✓ **Reducing exposure:** taking extra precautions can reduce the likelihood of harm occurring.
- ✓ **Training:** raising awareness at collection sites can assist with identifying and managing risks.
- ✓ **Monitoring:** continuous monitoring can help identify appropriate safeguards to minimize the risk.



What happens if the risk–benefit ratio changes after data collection?

Data controllers should assess the new risks in relation to the benefits and explore feasible alternatives. If no alternative exists, all measures should be taken to minimize the risks and its adverse effects. If the high risk continues, the data processing should discontinue.

Data controllers should continue to weigh the risks and benefits throughout the life cycle of data processing.

Box 5 : Effective risk–benefit assessment

- ✓ Identifying whether limitations to privacy and confidentiality are acceptable in light of the reasonable expectations of data subjects. This requires communication with data subjects to determine their reasonable expectations.
- ✓ Determining whether the IOM project is of sufficient importance to justify limitations to the rights and interests of data subjects. The importance of the IOM project should be based on IOM's mandate and the prevailing circumstances surrounding the particular IOM project, e.g. protection of data subjects, action required by the international community, public interest, human rights abuses, natural disasters, etc.
- ✓ Determining whether the safety, health and discriminatory risks are reasonable in relation to the benefits and to what extent the risks can be minimized.
- ✓ Considering the special circumstances and vulnerabilities of data subjects and promoting sensitivity to gender, age, language, and the social, cultural or religious attitudes of the target population group or individual data subject.
- ✓ Ensuring that appropriate safeguards are included in the data collection process to protect the rights and well-being of data subjects who are likely to be vulnerable to coercion or undue influence such as, inter alia, minors, detained data subjects, pregnant women, the physically or mentally disabled, and data subjects who may be economically or educationally disadvantaged.
- ✓ Reviewing the balance between the risks and benefits at periodic intervals to account for the possibility of a shift in the risk–benefit ratio.
- ✓ Foreseeing adequate training of IOM staff and others involved in the data collection process and ensuring that they are familiar with risk control measures to reduce the probability of harm occurring.
- ✓ Analysing how the flow of personal data will impact on the rights and interests of data subjects throughout the life cycle of data processing.

Note: When implementing data security, the data controller should take appropriate action to ensure that security measures minimize risks and maximize benefits.

Illustration of risk assessment at different phases of data processing

Data collection:

Data controllers should weigh safety and security risks to determine the nature and extent of personal data to be collected from conflict-affected populations when, for example, assigning shelter, providing food and engaging in camp organization. After conducting a fair assessment, appropriate action should be implemented to reduce the likelihood of any risks occurring and to ensure that the benefits continue to outweigh the risks. IOM staff members should be briefed about necessary precautions that would reduce the likelihood of harm, and the collection process should be continuously monitored.

Data retention:

After registration, the benefits of storing personal data at camp sites and the risks associated with unauthorized disclosure should be taken into account to ensure that the personal data are stored in a safe location. Access to the storage site should be limited to authorized persons and appropriate data security measures should be implemented to prevent theft or unauthorized disclosure.

Who is the data controller?



Data controllers are individuals who are authorized to determine the manner in which personal data are handled.

An IOM project may require one or multiple data controllers depending on, inter alia, the nature and size of the project, available resources, staff capacity, project management strategies, specified purposes of data collection and data processing, and transfer conditions.

Data controllers may include:

- chiefs of missions;
- project managers;
- project developers;
- delegated persons;
- individuals representing authorized third parties.

EXAMPLE:

The authorized individual representing a research institution becomes a data controller upon transfer of personal data. He/she then has the power to make decisions that are necessary to meet the specified research purpose as defined in the transfer contract.



Data controllers should always put themselves in the shoes of the data subject and consider:

“How would a reasonable person, in the position of data subject, react to the data collection and data processing practices?”

1



PRINCIPLE 1: LAWFUL AND FAIR COLLECTION



PRINCIPLE 1: LAWFUL AND FAIR COLLECTION

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

The twin criteria of lawfulness and fairness are manifest in all the IOM principles and should not be limited to the collection of personal data. The collection phase is highlighted because it is the first step of data processing that involves the handling of personal data.

3. Lawfulness

The collection and processing of personal data should be in accordance with the IOM principles, which are based on relevant international instruments and standards. Compliance with national data protection legislation should not be automatic.

Whether or not IOM complies with national data protection legislation will depend on the circumstances of the particular case and whether the law in question is consistent with the IOM principles and guidelines. Guidance should be sought from LEG as situations arise, particularly in the event of conflict, inconsistencies or doubt.

It should be noted that compliance with relevant national data protection legislation should not detract from the Organization's privileges and immunities. IOM's privileges and immunities vary from country to country depending on the status agreement that IOM has with the government.



Advice from LEG should always be sought prior to assuming any obligations that may impact on IOM's status as an intergovernmental organization in any given country.⁵

In practice, data controllers should:

- Research current international standards and national data protection legislation in the country of operation.
- Check the consistency between national data protection legislation and the IOM principles and guidelines.
- Raise awareness and foster cooperation with



EXAMPLE:

On occasion, donor contracts may require compliance with national or supranational data protection standards. This is increasingly the case, for example, with European Union contracts. LEG will note any data protection obligations during the contract review phase and give guidance as to how to proceed depending on the circumstances.

Box 6: Legal considerations

- Compliance with international human rights law;
- National or supranational laws affecting the IOM Principles;
- IOM's privileges and immunities in the country of operation, if applicable;
- Consent and confidentiality clauses included in interview, registration and application forms, as well as transfer contracts;
- Relevant IOM principles reflected in written contracts with agents (service providers/consultants), donors, IOM partners, implementing partners, government agencies, academic institutions and other third parties.

⁵ Privileges and immunities of the Organization that are relevant to data protection/national law include: immunity from all forms of legal process (immunity from jurisdiction), inviolability of IOM archives and all documents owned or held by it, wherever located

governments, donors, IOM partners, implementing partners, agents (service providers/consultants) and other third parties.

- Assess the legal capacity and the ability of data subjects to provide consent.
- Consider practical constraints that may hinder obtaining consent.
- Always seek advice from LEG.

4. Fairness

The amount of personal data should be limited to what is necessary to fulfil the specified purpose of data collection and data processing.

This will depend on the:

- pressing and legitimate need of the IOM project; and
- proportionality between the amount of personal data collected and the goals of the IOM project.

The application of these two factors will vary from case to case, depending on the sensitivity of the personal data and the context in which data collection and data processing occur.



Personal data should always be collected on a “need to know” basis.

Prior to collection, data controllers should identify:

- categories of personal data that are necessary to fulfil the original specified purpose; and
- additional categories needed for foreseeable use that are compatible with the original specified purpose, and that are likely to occur during the life cycle of data processing.⁶

To ensure fairness, there should be robust guarantees of confidentiality throughout the data collection process, and the original specified purpose, additional specified purposes, and all foreseeable disclosures should be clearly explained to data subjects.

Box 7: Fairness considerations

- Restrict the amount of personal data to a necessary minimum by taking account of the pressing and legitimate need of the IOM project, and assessing the proportionality between the amount of personal data collected and the goals of the IOM project.
- Create a legitimate expectation of confidentiality by giving clear indication and explanation of:
 - the specified purposes of data collection and data processing;
 - the foreseeable use, internal flows within IOM, methods of storage and all foreseeable disclosures to third parties.
- Maximize fairness by taking account of social, cultural and religious attitudes, as well as environmental challenges.
- Ensure that collection methods are gender, culture and age sensitive.
- Minimize intrusiveness by using the least intrusive method of collection.
- Inform data subjects and project stakeholders about the IOM Principles.

Note: Always promote truthfulness and cooperation.

5. Collection process

Personal data should be collected as expeditiously as possible, in a non-intimidating manner and with due respect for the safety and dignity of data subjects.

⁶ The specified purposes should be clearly defined according to the scope and objectives of the particular IOM project. The foreseeable use should be defined according to the assistance that could be rendered to the data subject throughout the life cycle of data processing.

Continuous communication

Communication with data subjects should be encouraged at all stages of the data collection process. This will help engender broad community awareness and confidence in the IOM project.

Equal treatment

Gender, cultural and age sensitivity should be reflected in the data collection process and equal standards should apply to each data subject.

Differential treatment may be justified, if it is necessary to assess the needs of certain data subjects and in order to adequately explain the data collection process to data subjects.

Interviewers soliciting and collecting personal data should, at all times, respect the confidentiality of personal data. To the extent possible, personal data should be collected directly from the data subject on a “one-to-one” basis, i.e. directly from both men and women, as well as girls and boys.

Social, cultural, religious, age, linguistic, environmental and health factors, or simply impracticality, may, however, prevent direct interaction between the interviewer and the data subject.

In these exceptional circumstances, personal data may be collected from relatives, authorized community members or close associates. If there is a conflict between the representative and the data subject, the views of the data subject will prevail. In all cases the best interests of the data subject remains paramount.

If exceptional circumstances preclude the presence of data subjects at collection sites, appropriate steps should be taken to ensure that data subjects validate their personal data as soon as it is reasonably practical.



EXAMPLE:

When collecting large quantities of personal data, focus group discussions could, for example, assist in identifying the range of community beliefs, ideas and opinions within the target population group. These discussions can serve the dual purpose of improving adherence to data protection, as well as improving the truthfulness and quality of personal data.



EXAMPLE:

With due consideration for family unity, dividing members of a large target population group according to sex and age could prove to be an efficient strategy for assessing needs and identifying suitable methods of collection. After parameters are defined and needs are assessed, the collection procedure has to be equitable and fair.



EXAMPLE:

In natural disasters, personal data may be collected from authorized representatives, such as the head of family or alternative family and community leaders. However, the personal data collected from representatives should be verified with the data subject as soon as the imminent danger has subsided and it is possible to arrange community meetings or spot checks.

Method of data collection

Personal data should be collected in a safe and secure environment and data controllers should take all necessary steps to ensure that individual vulnerabilities and potential risks are not enhanced.

The method of data collection will vary depending on the:

- specific context;
- type of IOM project;
- assistance required;
- project management strategies;
- staff capacity; and
- available resources.

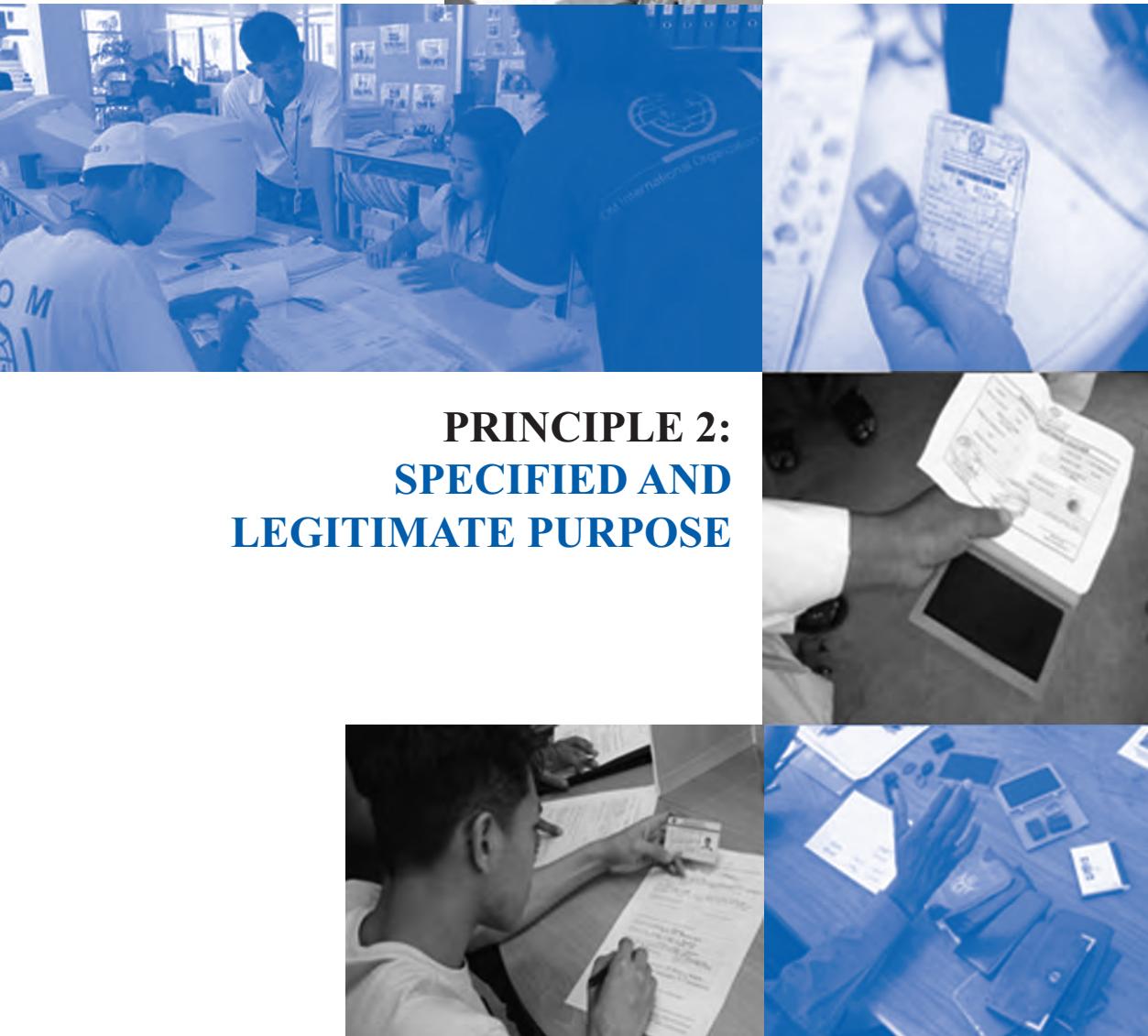
Data controllers should choose the most appropriate method of data collection that will enhance efficiency and protect the confidentiality of the personal data collected.



EXAMPLE:

In emergency situations, the collection of personal data rarely occurs at the initial phase of the emergency and when it commences, four phases may be identified: 1) planning, organization and migrant information campaigning; 2) fixing the population by distributing tokens necessary for issuing registration cards; 3) collecting detailed information, documentation and issuing registration cards; and 4) analysis, verification and information update. Depending on the specific context, project management strategies, available resources and staff capacity, mobile registration kits could be used as an on-site data capturing method during the third phase.

2



PRINCIPLE 2: SPECIFIED AND LEGITIMATE PURPOSE

PRINCIPLE 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).

The collection of personal data should not be indiscriminate and data subjects should be provided with a clear explanation of the specified purpose of data collection and data processing.

6. Specified legitimate purpose

The specified purpose should be clearly defined and justified by the necessity of fulfilling the legitimate need of the IOM project. The legitimate need should be determined by the data controller who takes account of the goals of the IOM project and the interests that it seeks to promote.



Personal data should only be used to fulfil the specified purpose(s) and it should not be subsequently used for unrelated purposes, without the consent of the data subject.

This limitation is a core principle of data protection that seeks to promote fairness and prevent a “functional creep”, i.e. additional uses of personal data which deviate from the original stated purpose and the expectations of the data subject.

The original purpose and additional foreseeable purposes should be defined and documented prior to data collection. This will help data controllers to identify the necessary categories of personal data needed.

The specified purpose should always yield added value and personal data should be used to support the dignity and autonomy of data subjects.

EXAMPLE:

The use of biometric data should be limited to the stated purpose. The specified purpose of State security should not lead to the arbitrary use of biometric data because it could result in unfair discrimination or limit the free and lawful movement of migrants.

Data subjects should be informed about any possible consequences of withholding categories of personal data, including the potential impact on service delivery and assistance that could be rendered to them.



Interview, registration and application forms should include a clause outlining the specified purposes and the content of the form should be clearly explained to data subjects at the time of data collection.⁷

⁷ See Template 1.2 containing a sample of a beneficiary's authorization for participation in IOM projects.

Data subjects should be notified if the original specified purpose subsequently alters due to unforeseen circumstances.

The degree to which the specified purpose has changed will determine whether notification is sufficient to continue with the data processing activities.

- ✓ **Insignificant change:** Despite the change, the data processing continues to be compatible with the original specified purpose.
- ✓ **Significant change:** Further data processing requires the subsequent consent of the data subject. In these circumstances, data controllers should only continue processing the personal data of those data subjects who provided consent for the new specified purpose.

EXAMPLE:

If it is impractical to contact the data subject, all reasonable steps should be taken to generally communicate significant changes to the target population group, for example, through public campaigning, radio broadcast, publications on the Internet or distributing pamphlets.

7. Compatible secondary purposes



Compatible secondary purposes refer to the use of personal data for purposes that are related to the original specified purpose.

These purposes are based on the need to fulfil the original specified purpose and include unforeseen purposes closely connected to the original specified purpose.

Data subjects should be made aware that their personal data could be used and disclosed for related purposes that aim to fulfil the original specified purpose.



Compatibility test

Evaluating whether it is reasonable to assume that data subjects would expect their personal data to be used in the proposed manner, even if the proposed use was not spelled out at the time of data collection.

To ensure compatibility, the secondary purpose must have a reasonable and direct connection to the original specified purpose.

Compatible secondary purposes that fall within the retention period may include:

- ✓ **Logistical and administrative purposes** that are necessary to achieve the original specified purpose.
- ✓ **Outsourcing project activities** to third parties that have a pre-existing relationship with IOM. This includes sharing personal data with unforeseen service providers.
- ✓ **Rendering continued assistance** within a particular IOM unit/department for the benefit

Box 8: Compatibility considerations

- Reasonable expectations of data subjects;
- Relationship between the original specified purpose and the secondary purpose;
- Nature and scope of personal data used or disclosed for the secondary purpose;
- Consequences on the rights and interests of data subjects;
- Extent to which suitable safeguards would protect the confidentiality of personal data and the anonymity of the data subject.

Note: Always limit the amount of personal data used and disclosed for secondary purposes to that which is necessary to carry out the specific related activity that is needed to fulfil the original specified purpose.

of the same data subject.

- ✓ **Tracing migration movements** if it is necessary to determine application for IOM assistance.
- ✓ **Specific case history analysis** if it is necessary to identify the vulnerabilities of data subjects.
- ✓ **Migration research and analysis** that promote IOM's expertise in migration issues and which fall within the defined migration research categories listed below.

EXAMPLE:

Analysing specific case history and tracing the migration movement of an individual data subject for the purpose of assessing whether he/she has benefited from multiple assistance voluntary return projects, would be a compatible secondary purpose.

8. Continuum of assistance



Continuum of assistance refers to the subsequent use of personal data for the benefit of the same data subject.

These additional purposes should be defined and explained to data subjects at the time of data collection.



At the time of data collection, data controllers should seek to obtain consent for a continuum of assistance.

In the absence of consent, the matter should be referred to LEG and the relevant IOM unit/department, particularly if data controllers believe on reasonable grounds that the use of personal data for a subsequent purpose would be necessary to protect the life or safety of the data subject.

9. Compatible research



Data matching

Data matching is the electronic comparison of two or more sets of personal data that have been collected for different specified purposes.

Internal data matching within the Organization may be allowed, if consent was obtained at the time of data collection, or if it is compatible with the original specified purposes for which the personal data were collected and processed.

Data controllers should always:

- assess the feasibility of the proposed data match;
- analyse the potential impact on the IOM principles; and
- undertake necessary safeguards to limit access, use and disclosure of personal data.

Central database applications that are used to store

EXAMPLE:

If MiMOSA (Migrant Management Operational System Application) is used to compare and clarify inconsistent personal data, the internal data match should be limited to the purpose of clarifying discrepancies between the two independent data sets.

personal data collected from independent IOM projects should be strictly monitored to ensure high levels of access controls and to prevent the misuse of personal data for arbitrary data matching purposes.

Personal data should not be disclosed to third parties for the purpose of data matching, unless it is explicitly and contractually defined, and the IOM principles are strictly adhered to by all contracting parties.

Migration research within IOM

The use of personal data by IOM for research relating to migration and analysis may be permitted, if it falls within the retention period, and if data controllers set strict conditions of access and disclosure.

The following migration research categories⁸ conducted by IOM are considered to be compatible for the purpose of the IOM principles and thus do not require further consent from the data subject.

- ✓ Advancing the understanding of migration realities and analysing the root causes of migration.
- ✓ Promoting best practices and upholding the human dignity and well-being of migrants.
- ✓ Encouraging social and economic development aimed at maximizing migration benefits.
- ✓ Providing expert advice to stakeholders and facilitating cooperation on migration matters.
- ✓ Assisting to meet the growing operational challenges of migration management.



EXAMPLE:

For the purpose of identifying migration trends in a certain geographical region, the IOM project manager of a new research/survey project should request access and use of personal data from the data controller responsible for handling the personal data required. The data controller will conduct a risk-benefit assessment to decide whether access should be granted. If the benefits outweigh the risks, the data controller should set appropriate access controls and limitation on further use vis-à-vis unauthorized IOM staff.

In practice, the following steps should be followed:

- A request by the IOM researcher specifying the migration research purpose should be submitted to the data controller involved in the IOM project for which the personal data were initially collected and processed.
- The initial data controller should conduct a risk–benefit assessment to determine whether or not authorization should be granted for access and use of the personal data.
- The initial data controller should determine whether the research request falls within the above noted migration research categories and thus would be considered a “compatible” purpose for which the consent of the data subject is not required.
- The confidentiality of personal data and anonymity of data subjects should be maintained when publishing research findings and analysis.

⁸ These categories are defined in terms of the IOM strategy and objectives. For further reference, see 2010 *Migration Initiatives*, IOM, Geneva.



10. Additional research purpose

Any additional research purposes that do not fall within the above noted migration research categories will require the subsequent consent of the data subject, if such consent was not obtained at the time of data collection.



If known prior to data collection, additional research purposes should be included in interview, registration and application forms.

The transfer conditions outlined in Principle 5 will apply to all additional research projects using personal data collected by a particular IOM project that do not fall within the above noted migration research categories. Furthermore, such additional research projects will require the approval of the data controller involved in the IOM project for which the personal data were initially collected and processed, as well as the relevant IOM unit/department.

Data controllers involved in research projects should ensure that the research has a clear focus and that the IOM principles are not compromised. Appropriate research methodologies should be adopted in coordination with the Research Unit at Headquarters to ensure that the accuracy and validity of the research study is not compromised by methods used to safeguard confidentiality.

The *IOM Research Manual*⁹ provides guidance on ethical principles to be considered when conducting research, implementing project management strategies and writing project reports.

Researchers should incorporate data protection into research methodologies to prevent risks and potential breach of confidentiality that may result from, inter alia, behavioural, social, biomedical and epidemiological research.

It may be useful to appoint designated persons to oversee research proposals and ensure conformity with any relevant ethical standards associated with various IOM activities.

Box 9: Research considerations

- Minimize physical harm, as well as social and psychological distress.
- Ensure honesty and transparency.
- Give a clear description of the nature of the research, the expected role of data subjects and the research methodology chosen.
- Treat data subjects as autonomous research subjects.
- Describe the specified purpose of the research and the broader objectives in a clear and intelligible manner.
- Obtain voluntary explicit consent at the time of data collection or as soon as the specified research purpose has been identified. Consent should be obtained in the form of writing, if feasible.
- Maintain confidentiality of personal data and anonymity of data subjects when publishing research findings and analysis.
- Promote the use of safe data security measures that are commensurate with the research methodology adopted.
- Ensure that data protection is applied throughout the research project.



EXAMPLE:

Ethical principles are included in various disciplines, for example: medical ethics require physician-patient confidentiality; direct assistance for trafficked persons requires individualized treatment and care; media ethics require accuracy and source validation; and research ethics require prevention of adverse consequences that could result from participation in the research study.

⁹ For further reference on research ethics, see 2004 *IOM Research Manual*, IOM, Geneva.

Research proposals

Analysis for the purpose of developing research proposals should be limited to anonymous data, if feasible. The use of personal data in project development strategies will require the explicit consent of data subjects, unless such use is compatible with the original specified purpose or subsequent specified purposes for which consent was obtained.



IOM staff and authorized third parties who conduct research using personal data collected by or on behalf of IOM should sign confidentiality forms.

A confidentiality undertaking is a necessary safeguard that seeks to:

- protect the anonymity of data subjects;
- safeguard the confidentiality of personal data; and
- ensure that identifiable factors are not used for arbitrary purposes.

The explicit consent of the data subject will be required for disclosure of personal data to third parties that are not involved in research projects.¹⁰



EXAMPLE:

Donors and IOM partners involved in research projects should be made aware of the IOM principles during the project development phase. This will help to ensure that adequate safeguards are built into research projects and that contractual terms do not compromise data protection.

Public interest research

Research conducted for public interest purposes that was not part of the original specified purpose and that does not fall within the above noted migration research categories should be approved by LEG and the relevant IOM unit/department, which should weigh varying factors to determine whether public interest in the promotion of the research outweighs, to a significant degree, the right to privacy and confidentiality of the personal data.

Research publications

Research publications should, in their format and content, preclude the identification of data subjects. Disclosure of research analysis, to the extent possible, should be limited to anonymous data. Unless data subjects explicitly agree to identification, their anonymity should be maintained.



EXAMPLE:

All necessary steps should be taken to prevent tracing the source of the research, for example, names could be protected by pseudonyms, and other identifiable factors could be substituted with fictitious data.

¹⁰ Disclosure to third parties should be limited to a minimum. See Principle 5 outlining the three strict conditions for transfer to third parties, i.e. explicit consent of data subjects, specified purpose of transfer and adequate safeguard measures.

3



PRINCIPLE 3: DATA QUALITY



PRINCIPLE 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.

Personal data should be of sufficient quality and quantity to meet the specified purposes. The amount of personal data collected should not exceed what is objectively necessary to fulfil the specified purposes.

Objective necessity depends on the:

- objectives of the particular IOM project;
- nature and scope of the personal data needed to fulfil the specified purposes; and
- expectations of data subjects.

Additional categories of personal data may be collected if the subsequent use is compatible with the original specified purpose, or if consent was obtained for a future specified purpose. The future specified purpose should be based on a continuum of assistance for the benefit of the data subject.

11. Measures to ensure accuracy

Accuracy is required throughout the life cycle of data processing, and should be checked at the collection, registration, retrieval, usage and disclosure phases. The frequency of checking personal data will depend on staff capacity and regular training to ensure that personal data are accurately recorded at the various stages of data processing.

The IOM Field Office involved in the collection and processing of personal data will remain the reference point for any significant changes, if personal data are stored in central database repositories.

Data controllers should create a “culture of meticulous checking” because incorrect recording of personal data may have an impact on service delivery. Reasonable steps should be taken to minimize the possibility of making a decision based on inappropriate and incorrect data.



EXAMPLE:

Collecting educational and employment history may not be relevant for the processing of assisted voluntary return applications, but it could be used for supplementary reintegration assistance, such as vocational training.



EXAMPLE:

Personal data stored in the Counter-Trafficking Module (CTM) database should be corrected by authorized IOM staff at the relevant IOM Field Office upon instruction from the data controller. IOM staff responsible for maintaining the CTM database should be notified of all significant changes.



EXAMPLE:

If host countries have restrictions based on medical conditions, the incorrect recording of HIV status could, for example, have an impact on the clearance procedure of resettlement applications.

Means by which to check accuracy may include the following:

- ✓ **Monitoring** the collection procedure.
- ✓ **Validating** the categories of personal data.
- ✓ **Cross-checking** prior to recording and when converting paper records to electronic formats.
- ✓ **Prior checking** before use and disclosure.
- ✓ **Regular reporting and continuous monitoring** throughout the life cycle of data processing.



To regularly monitor data quality, turnaround checklists should be circulated to IOM staff and authorized third parties handling personal data.¹¹

Integrity and truthfulness

Accuracy relates to the integrity and truthfulness of personal data. Interviewers should be trained to verify that the categories of personal data provided by data subjects, are true and correct.

If feasible, briefing sessions should be held prior to data collection to inform interviewers about the importance of obtaining and recording accurate personal data, and to ensure that participation in the data collection process does not expose data subjects to physical risks, intimidation or other threats that would cause the submission of false information.

Updates

Data controllers should afford data subjects the opportunity to update their personal data at any time. Any significant changes to personal data should be accurately reflected in paper and electronic records. All IOM staff and authorized third parties handling personal data should be informed as soon as the data controller becomes aware of any significant changes to personal data.

Box 10: Reasonable steps to ensure accuracy

- Assure data subjects that their personal data will be treated with the utmost care and confidentiality.
- Explain the consequences of providing incorrect personal data.
- Verify truthfulness and check accuracy at the time of data collection.
- Review categories of personal data and accuracy when retrieving personal data.
- Check accuracy prior to use and disclosure of personal data.
- Examine the format and medium of electronic records and transfer to compatible media.
- Coordinate with the relevant ITC officer to upgrade hardware and/or software devices.
- Examine the storage facility and volume of paper records and consider scanning, if cost effective.
- Produce quarterly or annual accuracy assessments depending on the length of the IOM project.
- Maintain inventories of paper and electronic records.

Note: Create a “culture of meticulous checking” and always allow data subjects to update and rectify their personal data at any time.



EXAMPLE:

To allow for updates, data subjects could receive notification to supplement, change or rectify their personal data within a defined period. This could be done by distributing pamphlets, publishing notices on the Internet and orally communicating the right to rectification and amendment when interacting with data subjects.

Technological compatibility

Electronic records should be kept in the most recent, current and accurate formats available. Outdated electronic media can cause corruption to the content of personal data and may lead to data loss due to technological obsolescence. Electronic media, hardware and/or software devices

¹¹ See Checklist 1 containing a model data quality turnaround checklist.



should be regularly updated and in line with IOM Information Technology and Telecommunications (ITC) Standards.

Data controllers should regularly review electronic media to ensure that personal data are in a readable format. Obsolete electronic tapes, diskettes, flash media and database applications should be updated to newer versions that are compatible with the latest information technology used at the relevant IOM Field Office.

EXAMPLE:

In accordance with ITC Standards IOM Field Offices should, for example, budget for the upgrade of hardware and/or software devices during the fourth year of the life cycle of the IT asset.

All outdated versions should be destroyed when no longer necessary. Electronic records should be regularly checked to reduce the risk of human error, and discrepancies and inaccuracies should be rectified by data controllers without undue delay.



Data controllers should maintain the integrity of electronic records by coordinating with the relevant ITC officer.

Safe paper-file storage

To protect the integrity of personal data, all paper records and verification documents should be securely stored in a locked safe, cabinet, drawer, or room to prevent wear and tear, forgery, manipulation or theft. Personal data that are archived or retained for back-up purposes will be regarded as accurate, provided that they are accurate at the time of storage.

EXAMPLE:

In the event of office relocation or closure, inventories could be used to mark paper files as “confidential” and to help ensure that all electronic records are encrypted for safe transfer to authorized staff at IOM regional offices or Headquarters, or to new premises.

Handover of personal data

The handover and movement of personal data should be carefully monitored to ensure that data quality and confidentiality are preserved at all times.



Data controllers should maintain inventories of electronic media and paper files that are used to store personal data.

These inventories will facilitate handover of personal data to new data controllers and may assist with management strategies for appropriate technical and organizational measures that are necessary for the safe and rapid movement of personal data. Relevant ITC officers could also use inventories when updating electronic media, database applications, and hardware and/or software devices.

12. Measures to ensure relevance

Data controllers should regularly assess whether categories of personal data are necessary and relevant. Inappropriate, obsolete or irrelevant personal data should be destroyed after consultation with the relevant IOM unit/department.



To determine continued relevance, “active data” may be separated from “inactive data.”

Sufficient reason should be provided for the continued relevance and retention of “inactive data”. This justification should be included in project reports or reports submitted for oversight purposes.



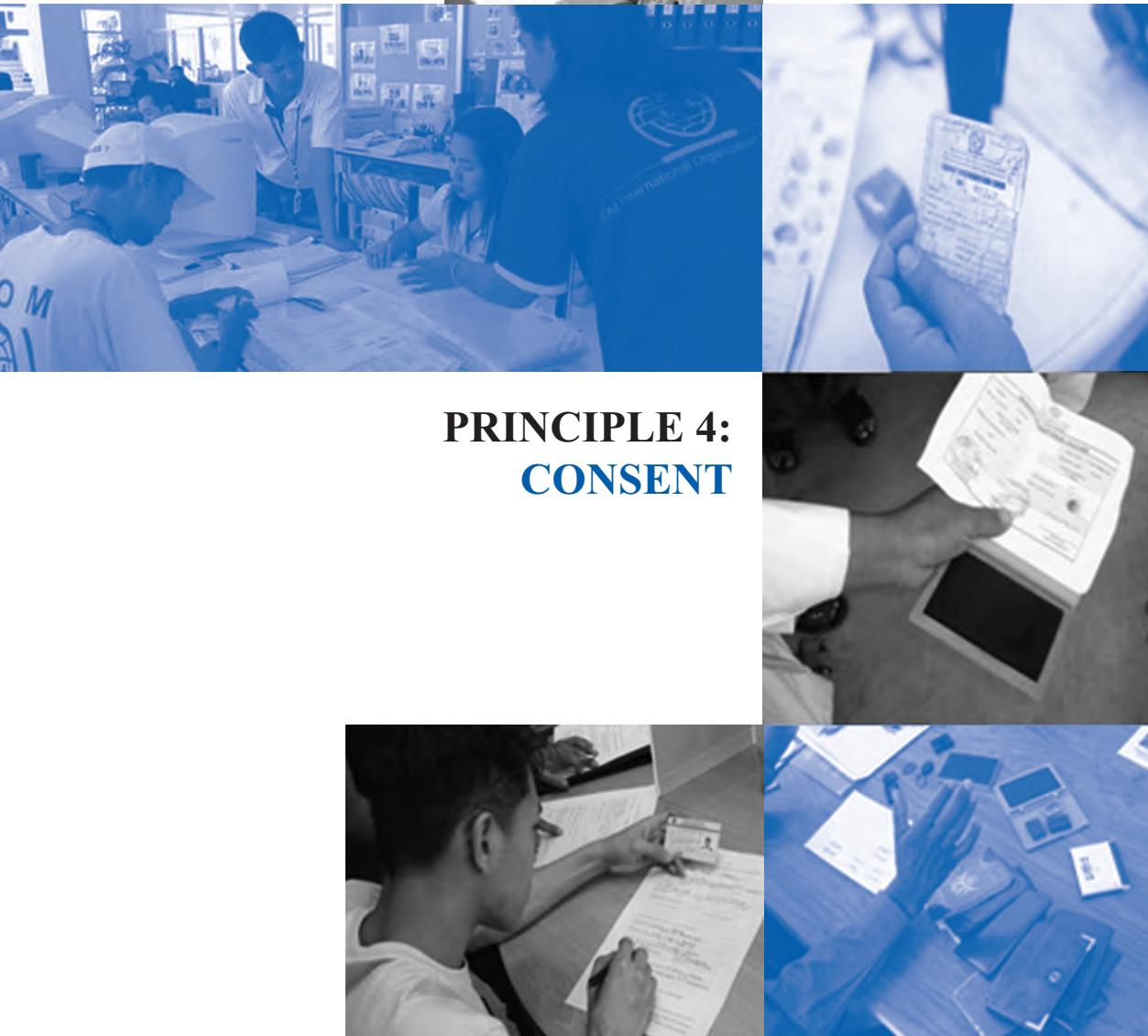
EXAMPLE:

“Inactive data” could be retained for a defined period to verify reparation claims. After the time period prescribed has lapsed, the “inactive data” should be destroyed if it is irrelevant or obsolete.

Box 11: Assessing continued relevance

- Have inaccuracies affected the quality of personal data?
- Have any updates and significant changes rendered the original record of personal data unnecessary?
- To what extent is the original record still capable of adding value to the objectives of the IOM project, and is it worth continued storage?
- Have the data subject’s circumstances changed, and do these new factors render the original record obsolete and irrelevant?
- Can “active data” be separated from “inactive data,” and has sufficient time elapsed to render the “inactive data” irrelevant?
- Can the irrelevant and unnecessary personal data be used for statistical or research purposes that are compatible with the specified purpose for which personal data were collected?

4



PRINCIPLE 4: CONSENT

PRINCIPLE 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.

Data subjects have the right to choose when and to whom they wish to reveal their personal data. Consent must be obtained from the data subject at the time of data collection, unless exceptional circumstances justify knowledge as the bare minimum requirement.

Data controllers should ensure that interviewers communicate sufficient information to data subjects, to allow for full understanding and appreciation of the specified purpose for which personal data are collected and processed. Sufficient knowledge may be presumed after all the relevant facts associated with the specified purpose, use and disclosure of personal data have been clearly explained to data subjects.

13. Capacity to consent



Capacity to consent refers to the ability to comprehend the implication of providing consent.

For consent to be valid, data subjects must have the capacity to consent. Children and mentally disabled data subjects should be interviewed in the presence of parents or legal guardians, and in the absence of either, advice should be sought from LEG. All capacity issues should be referred to LEG and the relevant IOM unit/department for guidance on how to proceed depending on the circumstances.

Forms of consent

The nature of the personal data and the surrounding circumstances of the particular IOM project will determine the form of consent that should be provided at the time of data collection.

- ✓ **Explicit consent:** an oral declaration or written signature provided by data subjects, indicating a clear understanding and appreciation of the implication of an expressed agreement that allows for data collection and data processing.

Box 12: Consent considerations

- Determine the legal, social and cultural capacity of data subjects.
- Consider physical ability and mental capacity to consent.
- Refer legal capacity issues to LEG prior to data collection.
- Map the internal flow of personal data within IOM and the foreseeable disclosures to third parties throughout the life cycle of data processing.
- Promote obtaining explicit consent in the form of writing.
- Incorporate consent clauses into existing interview, registration and application forms, or use a separate consent form at the time of data collection.
- Distribute notices when collecting personal data from large target population groups.
- Ensure that on-site electronic data capturing methods are accompanied by collective signing sheets.
- Explain access and complaint procedures (see Principle 7: Access and transparency).
- Provide IOM's contact details to data subjects at the time of data collection.

Note: Interviewers should be sufficiently trained. Gender, age, linguistic diversity, and literacy levels should always be taken into account.

- ✓ **Implicit consent:** no oral declaration or written signature is obtained, but the action or inaction of data subjects unequivocally indicates voluntary participation in the IOM project.
- ✓ **Proxy consent:** oral or written consent provided on behalf of data subjects by relatives, authorized community members or close associates in exceptional circumstances.



The form of consent should be recorded in interview, registration and application forms or electronic records.

If feasible, data controllers should seek explicit consent in the form of writing. Fingerprints or the data subject's mark (x) will be sufficient if data subjects are illiterate or unable to provide signatures.

The content of the consent form¹² and the consequence of a signature must be clearly explained in a language that allows for full appreciation and understanding of the specified purposes for which personal data are collected and processed.

Consent provided for the original specified purpose, additional specified purposes and disclosure to third parties, should be accurately recorded to allow data controllers to cross-check that consent was in fact obtained at the time of data collection.

Consent should be clearly reflected in databases applications in the event of conversion from paper records to electronic records.



EXAMPLE:

If paper records are manually uploaded to electronic format for storage in database modules, consent boxes should accurately reflect the form of consent and the categories of specified purposes for which consent was obtained.

14. Informed consent

Informed consent occurs when data subjects agree to the collection of their personal data after having considered all the relevant facts associated with data collection and data processing.



Data controllers should always consider potential language barriers and varying degrees of literacy levels.



EXAMPLE:

Printed sheets in A3 format outlining the specified purpose of data collection and data processing could be posted on walls or trees. Notification posters should be clearly explained to data subjects. If necessary, the use of megaphones, microphones, audiotapes or other means of voice projection should be used.

¹² See Template 1.1 containing a model consent form.

At the time of collection, data subjects should receive a clear explanation of the:

- specified and related purposes;
- any additional specified purposes, if known;
- necessary internal flows within IOM;
- access, correction and complaint procedures; and
- all foreseeable disclosures to third parties (including donors and project partners).

Obtaining consent for foreseeable disclosures to third parties and additional specified purposes at the time of collection will address potential practical difficulties of obtaining consent at a later date.

Withholding consent

All the relevant facts known to data controllers should be communicated to data subjects. This includes the benefit of providing consent and the risk of withholding consent, as well as any negative consequences that could result from disclosure to third parties.

If data subjects expressly withhold consent, they should be advised of the implications, including the effect it may have on assistance that could be rendered. If the data subject nevertheless makes an informed decision to withhold consent, the data collection should discontinue for that particular data subject.

Data subjects retain the right to withdraw consent at any stage of the data collection process. Data controllers should, to the extent possible, respect the wishes of data subjects and all related personal data should be destroyed after the withdrawal of consent.

15. Knowledge as the bare minimum requirement

Knowledge should only serve as the bare minimum requirement, if it is justified by exceptional circumstances. Data controllers should always weigh the risks and benefits to assess whether data collection should proceed on the basis of data subjects' knowledge alone.



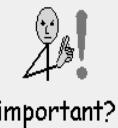
EXAMPLE:

In exceptional circumstances, personal data may be collected from the head of the family. If the wife disagrees with the husband who provided consent on her behalf, interviewers should reassure her about the IOM principles and explain the benefits of providing consent. If she persists to withhold consent, data processing should discontinue and all information relating to that individual data subject should be destroyed.



EXAMPLE:

Forced displacement as a result of armed conflict or natural disaster may leave thousands of people destitute. In these circumstances, it may be impractical to obtain consent in a timely manner. In the absence of consent, data subjects, at the very least, should be made aware of the reasons why their personal data are being collected. After the imminent danger has subsided, interviewers could, for example, obtain consent through information campaigning and circulation of collective signing sheets.



Data subjects should always be made aware of the specified purpose of data collection, even when exceptional circumstances preclude the timely provision of consent.

In these circumstances, data controllers should seek to obtain consent as soon as it is reasonably practical.

16. Proxy consent



Proxy consent is oral or written consent provided on behalf of the data subject by an authorized representative.

Data controllers should always consider any social, cultural, religious and environmental constraints that may prevent data subjects from providing consent.

In these situations, the consent of the head of the family may be taken as proxy consent. Data controllers should, however, use appropriate means to inform all family members of the specified purposes for which their personal data are sought and collected.



Proxy consent should only be permitted in exceptional circumstances, if it is impractical or inappropriate to obtain consent directly from the data subject.

17. Vulnerable data subjects



Vulnerable data subjects are individuals who may lack the legal, social, physical or mental capacity to provide consent.

Data controllers should always respect the vulnerability of certain target population groups and individual data subjects. Vulnerability will vary depending on the circumstances.

Respecting vulnerability involves balancing the social, cultural and religious norms of the group to which data subjects belong and ensuring that each data subject is treated as an equal participant in the data collection process.



EXAMPLE:

Data subjects may lack the social capacity to consent due to a cultural belief that elders always represent the interests of family members. If culturally appropriate, interviewers of the same sex should explain the specified purpose of data collection to ensure that each data subject understands the purpose and intended use of their personal data.

Box 13: Respecting vulnerability

- Promote gender, age and cultural sensitivity.
- Conduct focus group discussions.
- Encourage briefing sessions before and after data collection.
- Ensure that appropriate safeguards are in place to protect the rights and well-being of members of vulnerable groups and vulnerable individuals.

Vulnerability criteria may include:

- ✓ **Possession of particular characteristics** such as illiteracy, disability, age, etc.;
- ✓ **Location** such as detention facility, resettlement camp, remote area, etc.;
- ✓ **Environmental and other factors** such as unfamiliar surroundings, incomprehensible language and concepts, etc.;
- ✓ **Position in relation to others** such as member of minority group or sect, etc.;
- ✓ **Social, cultural and religious norms** of families, communities or other groups to which data subjects belong.

18. Gender sensitivity



Gender sensitivity involves the recognition of differences and inequalities while promoting the interests, needs and priorities of both men and women, as well as girls and boys.

In promoting gender sensitivity, data controllers should consider the social, cultural and religious norms of the group to which data subjects belong.

Both men and women interviewers should be sufficiently trained to ensure that gender sensitivity and power dynamics in family structures are equally weighed to prevent any negative repercussions that could result from participation in the data collection process.



EXAMPLE:

After assessing the power dynamics of the target population group, data controllers should, if feasible, ensure that women are interviewed separately by female interviewers who are trained to be sensitive to power dynamics, gender roles, family violence, etc.

Equal participation

The active participation of data subjects should be encouraged at all stages of the data collection process to allow individuals to express themselves freely in decisions that affect their lives. If feasible, interviewers should conduct breakaway discussion groups to explain the specified purpose for which their personal data are sought and collected.

Women and girls

The true spirit of informed consent may be negated by certain gender norms that often leave women and girls vulnerable to the undue influence of husbands, fathers, family members and community leaders. Data controllers should adopt a proactive approach to ensure that personal data are solicited and collected directly from women and girls.

Adolescent girls are often particularly vulnerable in situations of migration, due to assumed adult roles and social marginalization as a result of motherhood. The special roles of women and girls and the risk factors associated with participation in the data collection process should be identified prior to data collection, to ensure that appropriate measures are adopted during the data collection process.



19. Children



For the purposes of the IOM principles, children are data subjects under the age of 18 years.¹³

Legally, children do not have the capacity to consent. Parents or legal guardians should provide consent on their behalf and must, at all times, represent the best interests of the child.

The consent provided by parents or legal guardians may be negated if data controllers have sufficient reason to believe that they are acting contrary to the best interests of the child. In these circumstances, the conflict should be noted and advice should be sought from LEG.

Best interests of the child



The best interests of the child are paramount in all decisions affecting children.

Data controllers should always anticipate any adverse consequences that may result from collecting and processing personal data relating to children. Where necessary, data controllers should liaise with IOM partners to promote the best interests of the child.

The impact of conflicts, poverty and HIV/AIDS has eroded the traditional roles of children in certain communities, and has increased their vulnerability to exploitation and abuse.

Data controllers should determine whether children require special treatment as a result of trauma, particularly where children have been subjected to sexual exploitation and abuse, or where children have been victims of or have participated in armed conflict.



EXAMPLE:

If there is suspicion of parent involvement in inappropriate activities such as child trafficking, the matter should be referred to the relevant IOM unit/department and LEG for guidance.

Views and opinions of children



EXAMPLE:

Child counselling may assist with recording accurate case history that is necessary for rendering assistance to unaccompanied children.

Interviewers should be sufficiently trained to understand the different needs of girls and boys, as well as alternative family structures that may exist.

¹³ IOM recognizes 18 years as the upper benchmark for child protection. The protections under the 1989 Convention on the Rights of the Child extends to all persons under 18 years, even if majority is attained earlier under national law.



important?

The views and opinions of children should be respected at all times.¹⁴

The weight attached to the views and opinions of children will depend on the age and maturity level of the child.

Child participation should be fostered and data collection should occur in a child-friendly environment by interviewers of the same sex, if feasible.

EXAMPLE:

When communicating with children, the specified purpose of data collection should be explained in simple language, with the use of concepts appropriate to the child's age, stage of development and cultural background to facilitate understanding.

Guardianship

IOM cannot assume guardianship for children in the absence of parents or legal guardians, even if requested to do so by legitimate authorities.



important?

In the absence of parents or legal guardians, the matter should be referred to LEG.

In coordination with LEG, data controllers should consider appropriate procedures in the country of origin and/or host country for the appointment of a legal guardian. If necessary, data controllers should consult with IOM partners who specialize in the protection of children.

Special cases or projects where it is anticipated that there will be a substantial number of child-headed households, orphans or adolescents who assume the roles of adults, and cases of unaccompanied minors and separated children accompanied by adults who have assumed guardianship roles for the duration of travel, should be referred to LEG for guidance.

20. Elderly

The special needs of elderly data subjects should be considered when assessing the needs of target population groups.

Data controllers should assess physical and mental disabilities, as well as health-care and psychosocial needs, to ensure that adequate provision is made for elderly data subjects.



EXAMPLE:

When distributing food aid, separate registration booths could, if feasible, be allocated to elderly data subjects.

¹⁴ According to Article 12 of the 1989 Convention on the Rights of the Child, "A child who is capable of forming his or her own views has the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child." This principle is reiterated in the following instruments: 2007 Paris Principles and Guidelines on Children associated with Armed Forces and Armed Groups; 2005 Committee on the Rights of the Child General Comment No. 6 on the Treatment of Unaccompanied and Separated Children outside their Country of Origin; United Nations Children's Fund (UNICEF) Principles for Ethical Reporting on Children, available at: http://www.unicef.org/media/media_tools_guidelines.html; 2006 UNICEF Guidelines for the Protection of the Rights of Children Victims of Trafficking in Southern Europe; 1994 United Nations High Commissioner for Refugees (UNHCR) Refugee Children Guidelines on Protection and Care; and 2008 UNHCR Guidelines on Determining the Best Interests of the Child.



Interviewers should be sufficiently trained to ensure that elderly data subjects are not neglected during the data collection process.

21. Mental disability

Legally, mentally disabled data subjects are not capable of providing consent because they may not fully understand and appreciate the consequences of providing consent. Legal guardians should provide consent on their behalf. In the absence of legal guardians, data controllers should note the mental incapacity and seek guidance from LEG as to how to proceed depending on the circumstances.

22. Physical disability

Alternative measures should be provided for data subjects with physical disabilities and for the limited mobility of data subjects who may not be able to access data collection sites.



EXAMPLE:

Arm/hand amputee or deficiency may prevent written consent. In these circumstances, proxy signatures or oral consent should be recorded in interview, registration and application forms.

5



PRINCIPLE 5: TRANSFER TO THIRD PARTIES



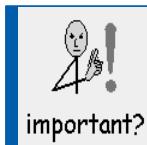
PRINCIPLE 5: TRANSFER TO THIRD PARTIES

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.

Sharing personal data with third parties should be strictly governed by a written contractual obligation to ensure that the transfer does not:

- compromise the IOM principles;
- undermine the confidentiality of personal data; or
- conflict with the reasonable expectations of data subjects.

Record of disclosures



Data controllers should maintain a record of all disclosures made to third parties.

Data subjects should, upon request and whenever practical, be provided with a copy of the record of disclosure relating to their personal data.

Records of disclosure should include the:

- name of data controllers;
- specified purpose of transfer;
- date of transfer; and
- description of the categories of personal data that have been disclosed.

23. Explicit consent

The explicit consent of the data subject is required for transfer of personal data to third parties, and all reasonable steps should be taken to obtain consent in the form of writing.



Transfer to all foreseeable third parties should be anticipated prior to data collection.

This will obviate the need to obtain consent at the time of transfer. Practical difficulties of obtaining explicit consent at the time of transfer may be taken into account, if it is reasonably

Box 14: Foreseeable third parties

- IOM staff that do not fall within the scope of the IOM project for which personal data were initially collected and processed.
- Agents such as service providers, consultants and researchers collecting personal data on behalf of IOM.
- Donors, IOM partners and implementing partners.
- Government agencies in countries of origin and host countries.
- Law enforcement agencies and government entities.
- Other third parties such as media, academic institutions, business, private companies, non-governmental organizations (NGOs) or unregistered organizations, international organizations and United Nations agencies.

Note: Always ensure that third parties explicitly agree to the IOM principles in writing. In the absence of commitment to adhere to the IOM principles, the matter should be referred to LEG.

justified. These exceptional cases should be referred to LEG who will provide guidance on a case by case basis.

24. Specified purpose of transfer

A request for transfer of personal data must be clear and specified and should include a description of the nature and categories of personal data needed, and the method of transfer to be used. All disclosures to third parties should be based on a “need to know” basis and only specific categories of personal data should be revealed to meet the specified purpose of the transfer request.

25. Adequate safeguards

Adequate safeguards that protect the confidentiality of personal data and the rights and interests of data subjects should be examined in light of the risks and benefits associated with the potential transfer. Data controllers should engage in a due diligence exercise taking account of all the circumstances surrounding the potential transfer.

Due diligence factors include:

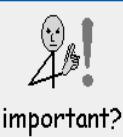
- ✓ the potential and actual risk to data subjects in the event of transfer;
- ✓ the nature of the personal data needed;
- ✓ the specified purpose for which personal data are requested;
- ✓ the duration of the proposed processing of the personal data;
- ✓ the type of entity requesting the transfer and its relationship with IOM;
- ✓ the laws applicable to the third party;
- ✓ the guarantee of respecting confidentiality of personal data and ensuring that the rights and interests of data subjects are protected during and after transfer.

Box 15: Indicators for written transfer contract

- Identify the contracting parties.
- Where necessary, assess the national data protection laws and regulations that would apply to the third party.
- Evaluate the country situation and respect for human rights and the safety of data subjects concerned.
- Consider whether it is necessary to share personal data or whether anonymous aggregate data will serve the specified purpose of the transfer request.
- List the nature and categories of personal data requested, and ensure that the amount of personal data is limited to that which is necessary to achieve the specified purpose of transfer.
- Identify the method of transfer, specify the conditions of transfer and ensure that the transmission process is safe and secure.
- Always keep the original records of personal data and provide a copy of the personal data necessary to meet the transfer request.
- Emphasize the importance of maintaining confidentiality of personal data and maintaining the anonymity of data subjects, and consider additional protection measures for vulnerable individuals.
- Include confidentiality/data protection clauses and attach the list of IOM data protection principles as an integral part of the contract.
- Only disclose to authorized persons and limit further use and disclosure vis-à-vis third parties that are not included in the written transfer contract.
- Outline necessary data security measures and access controls.
- Indicate the retention period and method of destruction after the specified purpose of transfer has been fulfilled.
- Determine whether IOM wishes to remain an anonymous source.
- Specify ownership and destruction of the personal data and highlight IOM's privileges and immunity, if applicable.

Note: Always seek advice from LEG and the relevant IOM unit/department.

The transfer of personal data should always be governed by a written contract.



Data controllers should weigh the risks and benefits prior to disclosure, to assess whether the third party would ensure comparable data protection measures during and after transfer.¹⁵

26. Method of transmission

In the event of transfer, appropriate measures should be used to safeguard the transmission of personal data to third parties. The method of transmission should be proportionate to the nature and sensitivity of personal data.

Secure methods of transmission include a combination of:

- ✓ **Encryption:** All electronic transmissions of personal data to third parties should be encrypted, where possible.
- ✓ **Confidentiality indicators:** E-mails containing personal data should only be sent on a “need to know” basis and it should generally be highlighted as “confidential” by using e-mail exchange applications, such as the Microsoft Outlook option, to identify the sensitivity of the e-mail
- ✓ **Courier/registered mail:** Posting encrypted CDs or confidential paper records should always be done via courier or, at a minimum, via registered mail and the envelope should be clearly marked as “confidential”.



The highest level of available encryption tools¹⁶ should be used to protect transfer of personal data to third parties.

27. Disclosures

All written transfer contracts¹⁷ should be referred to LEG for approval. Unless otherwise agreed, IOM should reserve the discretion to disclose personal data on a case-by-case basis.



Law enforcement agencies

Law enforcement agencies are national or international agencies that have legal authority to enforce or assist with the enforcement of the law.



EXAMPLE:

A request from EUROPOL to access personal data relating to trafficked persons for the purpose of combating trafficking in the European Union would require that the transfer of personal data take place in accordance with the three strict conditions of transfer, i.e. explicit consent, specified purpose of transfer and adequate safeguard measures.

¹⁵ The relevant IOM principles should be included in written contracts to promote the rights and interests of data subjects.

¹⁶ Data controllers should coordinate with the relevant ITC officer and consult with third parties prior to transfer, to ensure that they have compatible decryption tools.

¹⁷ See Template 2 outlining model contractual clauses for transfer to third parties.

Any request from national or international law enforcement agencies for access to personal data or access to IOM beneficiaries should be coordinated in advance with LEG and the relevant IOM unit/department. Disclosure of personal data for the purpose of criminal investigation and prosecution are subject to the approval of IOM and the data subject concerned. If applicable to the IOM project, existing relationships between IOM and law enforcement agencies should be communicated to data subjects at the time of data collection.



Agents

EXAMPLE:
A private company contracted to conduct registration activities could be an agent acting on behalf of IOM.

Agents are individuals or entities that are authorized to act on behalf of the data controller during the life cycle of data processing.

Agents are party to the specified purposes for which personal data are collected and processed and are directly authorized by IOM to assist with activities needed to fulfil the specified purposes. Data controllers should ensure that data subjects are aware of necessary disclosures to foreseen agents, as well as potential disclosure to agents that were not foreseen at the time of data collection.

Relationships between IOM and agents should be strictly governed by a written contractual obligation to ensure that agents adhere to the IOM principles and act upon the instruction of the data controller.¹⁸ The ownership of personal data should generally rest with IOM and the limitation on further use and disclosure vis-à-vis other third parties, as well as destruction of personal data, should be clearly defined in the contract of service.¹⁹



Implementing partners

EXAMPLE:
The United Nations High Commissioner for Refugees (UNHCR) and IOM working together to resettle a refugee could be implementing partners in a joint project.

Implementing partners are entities that work side by side with IOM in the execution of an IOM project activity.

A free flow of personal data may be permitted to entities that have a formalized relationship with IOM, if the transfer was foreseen at the time of data collection, and the data subject agreed to such transfer. Prior to transfer, data controllers should however, verify that the particular entity continues to satisfy the adequate safeguard condition of transfer.



IOM partners

EXAMPLE:
Awareness of the IOM principles should be raised at strategic meetings with host governments, United Nations agencies, international organizations, NGOs and members of target population groups involved in relief operations and camp management.

IOM partners are stakeholders that have a pre-existing agreement to work in cooperation and coordination with IOM.

Data controllers should liaise with all stakeholders to ensure that they are aware of IOM's

¹⁸ See Template 2 outlining model contractual clauses for contracts with agents.

¹⁹ See Template 2 outlining model clauses on data protection, confidentiality, ownership and destruction to be included in contracts.



commitment to data protection. This will help to engender cooperation for the implementation of the IOM principles.



Donors

Donors are persons or entities that contribute to the funding of an IOM project.

Data controllers should ensure that the IOM principles are not compromised by donor relationships. A useful method of raising awareness is to incorporate the IOM principles into project proposals under IOM policy considerations. Unless specified otherwise by donor requirements, IOM should assert ownership of personal data and incorporate an ownership clause into memorandums of understanding (MOUs) and donor agreements.²⁰ Donor reports should not include any personal data or photographs of vulnerable data subjects, unless prior written consent is obtained from the data subject.



If the three conditions of transfer have been met, the terms and conditions of transfer should be clearly defined in the written contract.

The ownership of personal data and adherence to the IOM principles should be incorporated into written agreements with third parties (see also Principle 11).

Media

IOM staff and authorized third parties should not speak to the media about specific cases that could lead to the identification of data subjects.²¹

All comments should be restricted to policy issues, unless they are authorized to disclose personal data.²² This is particularly important when dealing with vulnerable data subjects such as children, forcibly displaced persons, victims or assumed victims of human trafficking, and victims of physical and sexual violence.



EXAMPLE:
Without prior authorization, the name, material circumstances, photographs and case-specific details of victims of armed conflict should be withheld from reporters.

All data subjects have the right to remain anonymous with respect to media coverage, and the media should be encouraged to protect the identity of data subjects. Requests from the media to gain access to IOM beneficiaries or their personal data should be coordinated in advance with the Media and Communications Division and the relevant service area at IOM Headquarters. The request will be assessed on a case-by-case basis after determining the sensitivity of the case, the level of risk involved and the safety and best interests of the individual.

²⁰ See Template 2 outlining a model ownership clause/intellectual property clause.

²¹ For further details, contact the Media and Communications Division at IOM Headquarters.

²² Depending on the sensitivity of the personal data, the details of IOM staff or individuals representing third parties should not be revealed to the media without prior authorization. See Template 1.4 outlining a model media authorization form for data subjects.



If the beneficiary is a victim of human trafficking, additional considerations should be taken into account, including further safeguards to protect confidentiality and anonymity. The guiding principle of victim protection is to “do no harm”,²³ and this includes protecting the beneficiary from the media where there is a risk that the interaction will compromise his or her personal safety or rehabilitation. In addition, adequate time should be given to enable IOM to consider the request and, if appropriate, to identify a suitable individual who may be willing to participate in the media coverage.

IOM must always maintain the discretion to decide whether or not to facilitate access. Should IOM agree to facilitate access, prior written consent of the beneficiary should be obtained and the specified purpose of the request, as well as the specific risks and possible consequences of interacting with the media, should be clearly explained. Furthermore, IOM should sign an agreement with the media organization clearly describing the necessary protection standards, including, *inter alia*, strict compliance with the IOM principles is mandatory and highlighting the specific conditions of access according to the “Guidance note on media access to IOM beneficiaries who have been trafficked”.²⁴

Without prejudice to editorial independence, IOM should review and approve the final audio and video testimonial footage prior to distribution, airing or printing. IOM’s prior approval of the recording is necessary to ensure that adequate safeguards are in place to protect the image, voice and location of the beneficiary.



Unless prior consent is obtained, faces should be blurred, identities and location should be hidden, and voice-overs should be included in media coverage. This is particularly important for highly sensitive cases and vulnerable data subjects who may be at risk.

28. Photographs, video or audio, and digital footage

Photographs, video or audio, and digital footage of data subjects that are taken for the purpose of documenting and promoting IOM activities will require the consent of data subjects, whenever reasonably practical. Data subjects should be informed of the nature of the photo shoot or video and the purpose for which it will be used, including display in the IOM Image Library and future use in IOM’s work.²⁵

Highly sensitive cases will require the prior written consent of the data subject and, where appropriate, identities and locations should be hidden and faces should be blurred.

 **EXAMPLE:**
The faces of trafficked persons should not be displayed on television or in publication, unless said persons explicitly consent to it in writing.

²³ For further details on victim protection, see 2007 *IOM Handbook on Direct Assistance for Victims of Trafficking*, IOM, Geneva.

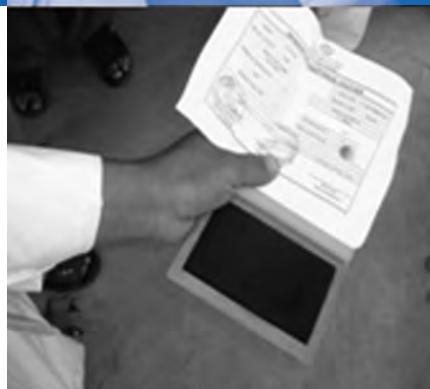
²⁴ For further assistance on the “Guidance note on media access to IOM beneficiaries who have been trafficked,” contact the Department of Migration Management, Migration Assistance Division at IOM Headquarters.

²⁵ See Template 1.3 containing a model photography consent form.

6



PRINCIPLE 6: CONFIDENTIALITY



PRINCIPLE 6: CONFIDENTIALITY

Confidentiality of personal data must be respected and applied at all 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 by confidentiality.

The confidentiality of personal data and the anonymity of data subjects must be respected throughout the life cycle of data processing.

29. Confidentiality commitment

Confidentiality pertains to the treatment of personal data that the data subject disclosed to IOM in a relationship of trust, with the expectation that the personal data would not be divulged in ways that are contrary to the wishes of the data subject.

Confidentiality should be used as a tool for cooperation and to ensure the truthful provision of personal data. A standard data protection clause²⁶ should be incorporated into existing interview, registration and application forms, or a separate confidentiality form should be used at the time of data collection to reinforce IOM's commitment to confidentiality.

Any limitation to confidentiality should be explained to data subjects at the time of data collection.

IOM's commitment to confidentiality should be promoted through briefings/training with, inter alia, IOM staff, agents (service providers/consultants), implementing partners, IOM partners, donors, countries of operation and host countries.

30. Confidentiality precautions

All IOM staff, agents, donors, IOM partners, implementing partners and authorized third parties should be briefed about the confidentiality of personal data prior to the collection, use and disclosure of such data.

Data controllers should take due care when authorizing the disclosure of personal data because

EXAMPLE:

If data subjects are selective in providing information as a result of mistrust, this may have an impact on the full range of support that IOM could provide for them. Data subjects should be reassured about IOM's commitment to confidentiality. This will help to engender confidence for the provision of true and correct information.

EXAMPLE:

Data subjects should be made aware of pre-existing information sharing agreements or donor requirements that may require the disclosure of certain categories of personal data to implementing partners and relevant countries involved in repatriation or resettlement projects.

²⁶ See Template 2.2 outlining a model data protection clause to be incorporated into interview, registration and application forms, where appropriate. The standard data protection clause should be included in contracts with agents (service providers/consultants), implementing partners, IOM partners, donors and other third parties.

breaches of confidentiality may result in a multitude of protection problems such as, *inter alia*, harm or threat to life, discriminatory treatment and detention.

IOM staff

All IOM staff are bound by the condition of confidentiality. This includes permanent, temporary and voluntary staff.



The undertaking to respect and maintain confidentiality of personal data should be guaranteed in writing.

IOM's standard clauses on data protection and confidentiality should be incorporated into all contracts of employment to ensure that personal data are protected at all times. The undertaking to respect confidentiality will continue to be valid after termination of employment.

Data controllers should ensure that confidentiality forms²⁷ are signed by all IOM staff who are authorized to handle personal data, particularly highly sensitive cases. This includes ITC staff, data-entry clerks, interns, researchers, formal and informal interpreters, designated counsellors and medical practitioners, as well as consultants.

The handling of highly sensitive personal data may require stricter safeguards. In such cases, guidance should be sought from the relevant service area/department.

Authorized third parties

All individuals representing authorized third parties are bound by the condition of confidentiality that will survive the expiration or termination of written contracts. Written contracts with third parties acting on behalf of IOM such as, *inter alia*, service providers, consultants, researchers and interpreters should clearly outline the duty to ensure the confidentiality of personal data and the responsibility to handle personal data in accordance with the IOM principles.

Box 16: Confidentiality considerations

- Implement continuous training with IOM staff and agents, and encourage joint training with service providers, implementing partners, IOM partners and donors.
- Be open and transparent and encourage a relationship of trust with data subjects.
- Assure data subjects about IOM's commitment to confidential treatment of their personal data.
- Explain the scope and limitations of confidentiality to data subjects at the time of data collection.
- Promote a "climate of confidentiality" in the office and with all authorized third parties.
- Ensure that personal data is treated with the utmost care and confidentiality throughout the life cycle of data processing.
- Authorize all disclosures in writing and ensure that authorized IOM staff and third parties understand the importance of maintaining confidentiality.
- Guarantee confidentiality by ensuring that confidentiality forms are signed.
- Apply strict access controls to authorized IOM staff and individuals representing authorized third parties.
- Maintain an access record of the categories of personal data disclosed.
- Highlight electronic and paper correspondence as "confidential," and ensure that recipients are carefully selected.
- Monitor the disposal of printed copies and other paper trails containing personal data.

Note: Refer uncertainties to the relevant IOM unit/department and LEG.



EXAMPLE:

Restricting access to certain categories of IOM staff, storing personal data in coded format, and transmitting personal data with higher levels of encryption tools may be necessary for the handling of highly sensitive personal data, such as medical data.

²⁷ See Template 3 outlining a model confidentiality form for IOM staff, interns and consultants handling personal data.

Data controllers should ensure that all third parties agree to the confidentiality condition prior to the transfer of personal data. A confidentiality clause²⁸ should be included in written transfer contracts with implementing partners, IOM partners, donors and other third parties that request access to personal data.

Data controllers should ensure that the confidentiality clause extends to IOM as a source,²⁹ if IOM wishes to remain anonymous in publications.



All written transfer contracts should include a confidentiality clause that should extend beyond the duration of the written contract.

²⁸ See Template 2 outlining a model confidentiality clause.

²⁹ See Template 2.1 outlining a model confidentiality clause covering the source of information.

7



PRINCIPLE 7: ACCESS AND TRANSPARENCY



PRINCIPLE 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.

Policy developments and practices should be transparent, and access, rectification and complaint procedures should be relatively straightforward.

31. Complaints

To allow for data protection complaints, the contact details of the relevant IOM Field Office should, at a minimum, be provided to data subjects at the time of data collection. The address, e-mail, telephone and fax number of the relevant IOM Field Office should be included in interview, registration and application forms, or distributed in leaflets at data collection sites.

Complaint procedures will vary depending, inter alia, on the:

- type of IOM project;
- nature of IOM activity;
- environmental factors;
- specific context;
- sensitivity of personal data;
- staff capacity; and
- available resources.

Box 17: Complaint considerations

- Allow data protection complaints in person, in writing or by telephone.
- Acknowledge and review all complaints.
- Protect the confidentiality of the complainant.
- Provide appropriate redress, if necessary.

Note: Always provide IOM's contact details to data subjects at the time of data collection.



EXAMPLE:

Cardboard complaint boxes could be made available at data collection sites, designated areas in resettlement camps or at IOM offices. If personal data are highly sensitive, and resources and staff capacity permit, an e-mailbox or hotline number could be used to receive data protection complaints from data subjects.

32. Access request from data subjects

All data subjects are entitled to access and rectify their personal data at any time, and data controllers should respond to access requests without undue delay. An access request from data subjects can be made in writing³⁰ or orally.

Disclosure of personal data should not be automatic. Data controllers should first consider all the prevailing circumstances surrounding the access request. These include, inter alia, the best interests of the data subject, absence of coercion, false identification, environmental factors,

³⁰ See Template 4 outlining a model access request form.

potential impact on the rights and interests of other data subjects, and safety of IOM staff and individuals representing authorized third parties.

Access to personal data should not be denied, unless it is clearly justified. Data controllers have the discretion to withhold certain categories of personal data, if immediate access would frustrate the specified purpose or assistance rendered to data subjects.



Data controllers should not reveal any information relating to data subjects, unless they are satisfied with the proof of identity.

The proof of identity from the data subject should be to the satisfaction of the data controller who reasonably believes that the data subject is who he/she purports to be. Registration cards or informal identification will suffice as proof of identity in situations where formal identification documents are unavailable.

Personal data should be communicated to data subjects in a clear and intelligible manner and on a “need to know” basis. Data controllers should only reveal summaries of individual cases or copies of categories of personal data to meet the purpose of the access request.

Any request to rectify or delete false or inaccurate personal data should be complied with. Significant alterations to personal data should be communicated to IOM staff and the authorized third parties who have access to personal data relating to the data subject. New information should be appended to existing electronic or paper records, and data controllers should attach a statement noting all corrections.

33. Access request from third parties

66

Disclosures to third parties are subject to the three strict conditions of transfer, i.e. explicit consent of data subjects, specified purpose of transfer and adequate safeguard measures (see Principle 5).



Data controllers should exercise common sense and due caution when responding to access requests from third parties.

Box 18: Access considerations

- Apply caution to access requests.
- Consider all the circumstances surrounding the access request.
- Only provide personal details to authorized representatives upon proof of identification.
- Only reveal categories of personal data on a “need to know” basis to meet the access request.
- Provide individual case summaries and/or copies of electronic or paper records.
- Accept requests to delete or rectify inaccurate personal data and inform IOM staff and authorized third parties handling personal data about significant changes.
- Maintain a record of access requests and the categories of personal data revealed.
- Provide clear justification for denying access in exceptional circumstances.

Note: The best interests of data subjects should be taken into account at all times.



EXAMPLE:

Brief oral summaries may be provided to meet specific access requests from data subjects in the aftermath of a conflict. Data controllers should, however, exercise due caution to prevent the disclosure of personal data under false pretence, particularly if the information could be used to harm data subjects and result in violence such as xenophobic attacks.



Parents and guardians

Requests from parents and legal guardians should be premised on the best interests of the child. Data controllers may refuse to reveal personal data relating to children, if they have sufficient reason to believe that it would be contrary to the best interests of the child. These cases should be coordinated with LEG and the relevant IOM unit/department.

Representatives

Requests from persons or entities representing the interests of data subjects should be subject to strict controls.



Data controllers should exercise careful discretion and should insist on valid identification, as well as oral or written proof of authorization from the data subject.

The legitimate interest of family members to seek family reunification and inquire about the whereabouts and well-being of data subjects should be weighed against the confidentiality of personal data and the rights and interests of data subjects.

Only non-personal data should be revealed to relatives and close associates, unless the data subject authorizes disclosure.

Advice should be sought from LEG if full disclosure is requested by relatives or close associates, without the consent of data subjects. Data controllers should check the authenticity of representatives with the information provided by the data subject and recorded in database applications or interview, registration and application forms.



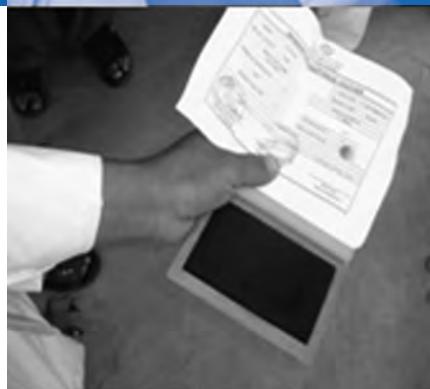
EXAMPLE:

In the absence of consent, and if there are no safety and security risks, disclosure to relatives and close associates should be limited to the fact that the person has been registered with IOM.

8



PRINCIPLE 8: DATA SECURITY



PRINCIPLE 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.

Data security



Data security is a set of physical and technological measures that safeguard the confidentiality and integrity of personal data and prevent unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

Data controllers should monitor the internal and external exchange of personal data to ensure that appropriate data security measures are applied to electronic and paper records.

Data security measures will vary depending, inter alia, on the:

- type of IOM project;
- nature of the personal data;
- format of storage medium;
- environment of the specific workstation; and
- technological capabilities at the relevant IOM field office.

A “culture of data security” should be adopted to guarantee safe and secure access, storage, transmission and destruction of personal data.

34. Data security risks

Data security risks should be approached by data controllers through systematic risk assessment³¹ and effective risk management practices.

Suitable physical and technological measures should be applied in coordination with the relevant ITC officer to reduce possible threats and vulnerabilities.



Data security measures should be routinely reviewed and upgraded to ensure a level of data protection that is adequate to the degree of sensitivity applied to personal data.

³¹ See Checklist 2 outlining a model data security assessment checklist to be used in conjunction with relevant ITC standards and policies.

35. Classification of records

A standard classification of records should be applied after assessing the sensitivity of personal data.³²

All electronic and paper records should be clearly marked to limit transmission to authorized IOM staff and individuals representing authorized third parties.

Classification of electronic and paper records:

- ✓ **Unrestricted dissemination:** anonymous aggregate data³³ generally disseminated within the Organization and that may be publicized and disclosed to third parties.
- ✓ **Restricted dissemination:** limiting disclosure of non-personal data to the following internal flows within IOM:
 - non-personal data disclosed within the Organization for IOM internal use, for example, statistical reports and inter-office memorandums;
 - non-personal data limited to internal IOM unit/departmental use within the Organization and restricted from general IOM dissemination, for example, project-specific analysis and case reports.
- ✓ **Confidential:** all personal data that data subjects disclosed to IOM in a relationship of trust.
- ✓ **Secret:** highly sensitive personal data³⁴ relating to specific data subjects that could cause serious repercussions and could violate human rights, if disseminated.

Box 19: “Culture of data security” indicators

- Conduct a data security risk assessment.
- Review and assess data security measures at regular intervals.
- Raise awareness about data security risks.
- Foster greater confidence in the use of data security measures.
- Promote cooperation among IOM staff, and with agents (service providers/consultants), implementing partners, IOM partners, donors and other third parties.
- Use strict access controls, confidentiality indicators and encryption tools, and maintain an access record of IOM staff and third parties authorized to handle personal data.
- Report any suspicious activity to the relevant ITC officer.
- Respond to security incidents in a timely manner.
- Consider data security in project development strategies and include necessary costs in project proposals.
- Ensure that an inventory of equipment and electronic storage areas are kept and share it with the relevant ITC officer.
- Cooperate with the ITC department at Headquarters to ensure that appropriate data security measures are applied to personal data throughout the life cycle of data processing.

Note: Stricter data security measures may be necessary for access, storage and transmission of highly sensitive personal data.

36. Physical security measures

The safeguard measures outlined in relevant IOM information technology (IT) policies and guidelines should be followed by all IOM staff handling personal data.

³² The sensitivity assessment should be conducted prior to data collection. For further details, see the introductory section.

³³ Anonymous data will fall within the scope of the IOM principles until such time that the personal data to which it relates have been effectively destroyed.

³⁴ Highly sensitive personal data are personal data and material circumstances that could be used to harm or threaten the life of data subjects and IOM staff or agents, or substantially affect the rights and interests of the data subject. The level of sensitivity applied to personal data will depend on the sensitivity assessment that should be conducted prior to data collection.

Paper records



important?

Paper records should be posted via the most secure means available at the relevant IOM Field Office to avoid unauthorized access, accidental loss or theft.

Secure methods of posting paper records include:

- courier or, at a minimum, registered mail;
- converting paper records to electronic format:
 - scanning paper records to electronic format and posting encrypted electronic media by courier or registered mail; or
 - scanning paper records and posting encrypted data in a secure FTP³⁵ site, i.e. exchange of personal data from one computer to another using secure Internet exchange application protocols.

Electronic records

Electronic records and equipment such as CDs, DVDs, flash memory, microfiches, videotapes, audio tape backups and other electronic storage media containing personal data should be kept in a safe location to prevent physical damage, unauthorized access and modification.

Effective physical safeguards include:

- ✓ Classifying records according to the appropriate level of sensitivity;
- ✓ Restricting access to buildings, offices, and shelters to authorized staff with a legitimate duty need;
- ✓ Securing access to storage premises by requesting identification cards;
- ✓ Separating personal data from non-personal data;
- ✓ Ensuring that paper records are stored in locked safes, shelves, drawers, filing cabinets or rooms, and returning paper records to secure locations after use;
- ✓ Monitoring printers used to produce personal data and ensuring that appropriate methods of disposal are used to destroy printed copies, such as shredding or burning;

EXAMPLE:

Posting sensitive paper records relating to irregular migrants may require conversion from paper records to electronic records to protect personal data from “falling into the wrong hands” at airports. Data controllers could either: 1) scan the paper records to CDs and encrypt the CD for postage by courier or registered mail, or 2) convert the paper records to electronic format and use an FTP site as an archive system to exchange the personal data. Although FTP is password-protected, it does not automatically encrypt files. Data controllers should ensure that electronic records are encrypted prior to sharing the ftp address with authorized third parties.

EXAMPLE:

Access to central database repositories, such as MiMOSA or archives systems, should be password-protected and limited to authorized IOM staff.

³⁵ FTP (File Transfer Protocol) is an application protocol that can be used to exchange files between computer accounts, transfer files between an account and a desktop computer, or access archives on the Internet via an FTP address (similar to an http:// or website address, but uses the prefix ftp://). The hosting computer serves as a password-protected archive system to post and download files.



- ✓ Keeping a minimum number of backup copies in fire-rated safes and storing it in a separate location that allows for easy transportation in the event of evacuation or relocation;
- ✓ Ensuring that electronic records are stored in safe locations and limiting access to authorized IOM staff;
- ✓ Concealing archive files and limiting access to authorized IOM staff;
- ✓ Protecting the combination code of safes by restricting access and changing the code at regular intervals.

Social engineering

In data security, social engineering is a term used to describe deceptive techniques that are used to psychologically trick people into revealing personal data or security access codes.

Social engineers are people who engage in social engineering for the purpose of gaining unauthorized access to personal data.

Social engineers typically avoid the use of information technology and rely on:

- vulnerabilities of human nature;
- inability to keep up with a culture that relies heavily on information technology; and
- carelessness in protecting passwords.



EXAMPLE:

The social engineer may befriend someone who is authorized to access storage areas containing personal data and exploit his/her confidence to gain access to personal data. The social engineer will take advantage of the authorized person's natural inclination to choose passwords that are meaningful to him/her and easy to guess by a friend.



People are often seen as the “weak link” in a security system and no matter how safe and secure the data security measure, social engineers will try alternative means to take advantage of people.

Typical social engineering techniques may include:

- persuasion or manipulation;
- appeal to vanity;
- imitating someone in a position of authority;
- eavesdropping;
- “shoulder surfing”, i.e. looking over someone’s shoulder and memorizing passwords;
- “dumpster diving”, i.e. sifting through paper trash to find clues that can be used to unlock password protection;
- “phishing”, i.e. pretending to be a trustworthy electronic source in an attempt to maliciously acquire personal data.



Unintentional disclosure of information to social engineers may endanger the lives of data subjects, as well as IOM staff and individuals representing authorized third parties.



Data controllers should include social engineering in data security risk assessments and implement appropriate prevention strategies.

Prevention strategies may include:

- ✓ Raising awareness that social engineering is a technique used to compromise data security systems;
- ✓ Updating data security measures to address social engineering;
- ✓ Carefully selecting and protecting password entry;
- ✓ Keeping personal data strictly confidential;
- ✓ Avoiding disclosure of personal data via unsecured telephone lines;
- ✓ Requiring authorized access to premises;
- ✓ Monitoring the disposal of personal data;
- ✓ Shredding or burning highly sensitive personal data.

37. Technological security measures

Data controllers should ensure that strict access controls are used to safeguard electronic records. Computer systems, database applications and other software tools used to store electronic records should be limited to authorized IOM staff. All IOM staff, including ITC officers, should sign confidentiality forms to protect the confidentiality of personal data.³⁶



EXAMPLE:

ITC officers should sign confidentiality agreements and data protection should be included in the orientation on ITC code of conduct and IOM IT policies.



Encryption

Encryption is the process of converting text into incomprehensible code and using a key to protect the original format of the text.

Data controllers should encourage the widespread application of encryption tools, where possible. See Principle 10 for alternative methods of removing identifiable factors prior to transmission/disclosure.



EXAMPLE:

Built-in encryption tools within MS Office or WinZip applications should be used for internal transfer between IOM staff. A higher level of encryption, for example, PGP (Pretty Good Privacy), should be applied to highly sensitive personal data.

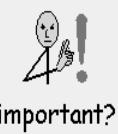
IOM staff handling personal data should coordinate with the relevant ITC officer to ensure that appropriate steps are taken to protect all electronic records prior to transmission, including through encryption.

Decryption keys should be allocated to data controllers or designated custodians and ITC officers to avoid operational hazards if keys are lost or misplaced, and if custodians are absent. Decryption keys should be safely stored at all times.

75

³⁶ See Template 3 outlining a model confidentiality form for IOM staff handling personal data. ITC officers should comply with ITC policies and guidelines and undertake to maintain confidentiality when accessing personal data.





Encryption is a necessary safeguard that should be used at all times to protect personal data from unauthorized access, modification, tampering or accidental loss.

All e-mail correspondence should be limited to authorized IOM staff on a “need to know” basis. Recipients of e-mail correspondence should be carefully selected to avoid general IOM dissemination of confidential and secret personal data.



Partial encryption

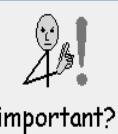
For the purpose of the IOM principles, partial encryption refers to the application of encryption to limited electronic storage areas, such as folders, files and database applications containing personal data.



EXAMPLE:

The internal transfer of individual case-specific indicators should only be sent to authorized IOM staff. E-mail recipients should be carefully chosen and the identity of data subjects should be substituted with IOM identity numbers if referred to in the body of e-mails. MS Excel templates containing core indicators should be encrypted with the appropriate encryption tools.

Partial encryption is a useful safeguard that should be used to protect electronic storage areas from unauthorized access, modification or tampering. Partial encryption may, however, provide a false sense of data security, and data controllers should ensure that encrypted folders or files are not mistakenly stored outside encrypted areas after retrieval.



Enhanced password protection should be used for access, storage and transmission of electronic records.

In the absence of encryption tools, pseudonyms, passwords and codes should be used to protect the confidentiality of personal data and the anonymity of data subjects (see Principle 10).

Security risks

Data controllers should coordinate with the relevant ITC officer to ensure that computer systems, applications and other software tools used to capture and store personal data are protected by antivirus, spyware and adware removal tools and a firewall.³⁷ If these are not available or functioning, the data controller should immediately contact the relevant ITC officer.

Loss and theft

ITC officers should take all reasonable steps to recover lost electronic folders or files containing personal data.

³⁷ This should be in accordance with IOM authorized security risk applications.





important?

All incidents of loss or theft should be reported to the relevant ITC officer without undue delay.

The safety procedures developed by the ITC department at Headquarters should be followed to prevent exposure to risks, such as patches or latest service packs.

Accessing the IOM server

Remote access to the IOM server and the use of home-based desktops or laptops should comply with the safety standards set out in the IOM IT Policies, IT Issues Regarding Home-Based Work and IOM Policy on Home-Based Work.

Electronic records containing personal data should not be processed or transmitted without adequate protection against malicious software.



important?

The use of Internet outlets and unsecured wireless connections to retrieve, exchange, transmit or transfer personal data, should be avoided.

IOM staff handling personal data should take due care when connecting to the IOM server from outside premises. Passwords should always be protected and they should check that they have logged-off properly from computer systems and that open browsers have been closed.

Laptops, Blackberries, PDAs and other portable media

Laptops, Blackberries, personal digital assistants (PDAs) and other portable media equipment, require special safety precautions, especially when working in a difficult environment. Data controllers should always ensure that electronic files containing personal data are password-protected and that password-protected features³⁸ are enabled. Portable media equipment should be stored in safe and secure locations at all times.

Box 20: Considerations for electronic records

- Only transmit and store personal data on computer systems and database applications that are protected against security risks.
- Use the login procedures and minimum requirements for password protection as indicated in the IOM IT policies.
- Use the automatic lock computer or log-off actions and ensure that all browsers are closed if workstations are unattended, especially in situations where computers are shared by several users.
- Highlight all e-mails containing personal data as “confidential” by using the Microsoft Outlook option or other e-mail exchange applications to identify the sensitivity of the e-mail.
- Limit e-mail recipients to authorized IOM staff and individuals representing authorized third parties.
- Substitute codes for identifiers when storing and transmitting personal data, particularly when handling categories of highly sensitive personal data.
- Always encrypt the transmission of e-mails and attachments containing personal data:
 - *Within IOM:* use built-in encryption tools within MS Office and WinZip applications, PGP or other encryption applications.
 - *Outside IOM:* use the highest level of encryption tools available and ensure that third parties have appropriate decryption tools.
- Use partial encryption to protect electronic storage areas and ensure that personal data are securely stored in encrypted or password-protected folders.
- Secure portable media and report loss or theft of electronic equipment without undue delay.
- Ensure that backup procedures are applied to all electronic records.
- Avoid accessing the IOM server via unsecure Internet outlets or wireless connection to retrieve, exchange, transmit or transfer personal data.

Note: Data controllers should coordinate with the relevant ITC officer to ensure that the highest level of encryption is used for transfer to third parties outside IOM because only pre-configured IOM equipment guarantees a safe exchange of information.

³⁸ For further guidance, coordinate with the ITC department at IOM Headquarters, particularly on application of IT policies and guidelines, and safety measures to be taken for the handling of portable media equipment.

Portable or removable devices should not be used to store highly sensitive personal data. If this is unavoidable, personal data should be transferred to appropriate computer systems and database applications as soon as it is reasonably practical. If flash memory such as USB flash drives and memory cards are used to temporarily store personal data, it should be kept safe and the electronic record must be encrypted. Guidance should be sought from the relevant ITC officer, where necessary.

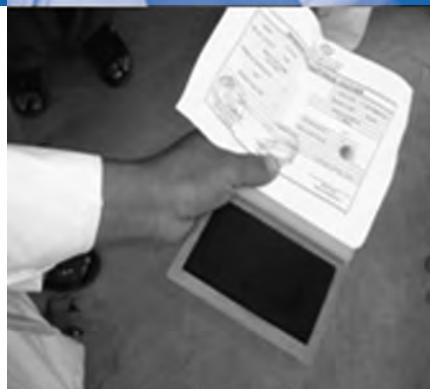
Recovery and backup

Effective recovery mechanisms and backup procedures should cover all electronic records, and the relevant ITC officer should ensure that backup procedures are done on a regular basis. The frequency of backup procedures will vary depending on the sensitivity of the personal data. Electronic records should be automated to allow for easy recovery in situations where backup procedures are difficult due to, inter alia, regular power outage, system failure or natural disaster. When electronic records and database applications are no longer needed, IOM staff should coordinate with the relevant ITC officer to ensure permanent elimination.

9



PRINCIPLE 9: RETENTION OF PERSONAL DATA



PRINCIPLE 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.

Data controllers should monitor retention and destruction of personal data because overzealous application of the retention principle may lead to premature destruction of personal data. Data controllers may delegate the retention monitoring role to authorized IOM staff responsible for maintaining access controls, preserving storage media, and reviewing whether records are readable and comprehensible.

38. Retention period

Retention of personal data is strictly related to the achievement of the specified purposes. The timescale for retention should be strictly adhered to and should be calculated from the date of completion of the IOM project.

Box 21: Retention period

- 10 years:** Electronic records containing personal data.
- 8 years:** Paper records containing personal data.

Note: Retention periods may, however, vary, depending on donor requirements.



Personal data should not be kept for an indeterminate period, and electronic and paper records, as well as respective backups, should be destroyed or rendered anonymous as soon as retention periods have expired.

The format in which personal data are kept will depend on the discretion of data controllers who should consider, inter alia, the:

- technological capabilities at the particular IOM Field Office;
- data security measures;
- access controls measures; and
- availability of space for storage.

Data controllers should ensure that the integrity and quality of electronic and paper records are maintained throughout the life cycle of data processing. Advice should be sought from the relevant ITC officer to ensure that all electronic records are compatible with the latest available information technology.



Personal data should be kept in safe and secure locations with appropriate confidentiality indicators and access control measures.

81

The electrical and fire safety standards outlined in the IOM IT Policies and Staff Security Unit (SSU) Guidelines should apply to storage locations. Storage volumes should be kept to a necessary minimum and only essential information should be retained.

Data controllers should assess whether duplicate electronic and paper records have been collected or recorded. If a scanner is available and the process of scanning is not unduly burdensome, paper records should be converted and retained in electronic format to reduce storage volumes.

The nature of personal data, climate conditions, and easy access to authorized IOM staff are relevant factors that should be taken into account when monitoring the storage of personal data.

39. Retention for additional specified period

Retention of personal data for additional specified purposes that are not related to the original specified purpose or compatible purposes will require the subsequent consent of data subjects.

The retention principle, however, creates an exception in situations where it would be in the best interests of the data subject to retain personal data beyond the fulfilment of the specified purposes of data processing.

Box 22: Further retention considerations

- Engage in a risk–benefit assessment.
- Define the additional specified purpose for the benefit of the data subject.
- Provide adequate justification for further retention.
- Define the time period for further retention.

In these circumstances, data controllers should:

- Identify the additional specified purpose for the benefit of data subjects.
- Define the period of further retention in accordance with the nature of the IOM project and the benefit of further retention.
- Conduct a risk–benefit assessment.
- Coordinate with the relevant IOM unit/department to determine whether data subjects would reasonably expect IOM to use their personal data for the additional specified period.

The retention period may be exceeded in circumstances where it is necessary to retain personal data for IOM organizational use such as:

- monitoring and evaluation;
- case history analysis;
- mapping migration trends or patterns; and
- statistical analysis.



EXAMPLE:

The data subject could be the beneficiary of a subsequent IOM project and destroying the personal data would not only be disproportionate to the interests of the data subject, but also costly and onerous to IOM.



Data controllers should submit retention assessment reports to the relevant IOM unit/department to justify further retention.

All extensions to the retention period should be approved by the relevant IOM unit/department.

40. Destruction methods

Data controllers should consider whether personal data could be used for analytical or research purposes before authorizing destruction.

When no longer necessary, all records and backups should be destroyed or rendered anonymous.



Destruction of electronic and paper records should be authorized by the data controller in coordination with the relevant IOM unit/department.

The method of destruction will depend, inter alia, on the:

- nature and sensitivity of the personal data;
- format and storage medium; and
- volume of electronic and paper records.

Data controllers should conduct a sensitivity assessment prior to destruction to ensure that appropriate methods of destruction are used to eliminate personal data.

Destruction of paper records

Paper records should be destroyed by using methods such as shredding or burning, which do not allow for future use or reconstruction. Waste disposal and burial should be avoided.

After accurately converting paper records to electronic format, all traces of paper records should be destroyed.

Destruction of electronic records

The destruction of electronic records should be referred to the relevant ITC officer because the delete features on computer systems do not necessarily ensure complete elimination.

Donation of computers and electronic equipment, if authorized by the donor of the IOM project, should be done by way of a deed of donation.

Box 23: Destruction considerations

- Consider the possibility of further use in accordance with the IOM principles, prior to destruction.
- Be confident that the personal data will not be needed for organizational purposes, such as statistical use or monitoring and evaluation.
- Ensure that destruction decisions are approved by the relevant IOM unit/department.
- Conduct a sensitivity assessment and submit a categorized list of electronic storage areas to the relevant ITC officer.
- Coordinate with the ITC department to ensure that appropriate destruction methods are used to destroy electronic records.
- Monitor physical methods of destruction.
- Ensure that outsourcing for destruction purposes are governed by written contracts upholding the confidentiality of personal data and ensuring the submission of certification of destruction.
- Monitor electronic destruction until final elimination.
- Attach disposal records to final project or evaluation reports.
- Include destruction of personal data in contracts with third parties, and request certification that all copies have been destroyed after termination or expiration of the contract.

Note: Ensure that third parties submit disposal reports and certification of destruction, particularly if the destruction of personal data is outsourced.



EXAMPLE:

If personal data are encoded and uploaded by data-entry clerks into database modules, the data controllers should authorize destruction, if appropriate and after satisfaction that the personal data have been accurately recorded.

Prior to donation, the data controller should coordinate with the relevant ITC officer to ensure that all traces of personal data are completely eliminated.

Upon instruction, the relevant ITC officer should ensure that all traces of personal data are completely removed from computer systems and other software. Disk drives and database applications should be purged and all rewritable media such as, inter alia, CDs, DVDs, microfiches, videotapes, and audio tapes that are used to store personal data should be erased before reuse.³⁹ Physical measures of destroying electronic records such as recycling, pulverizing or burning should be strictly monitored.

EXAMPLE:

The ITC department should ensure that electronic records containing personal data are completely destroyed before donation or sale of computers. If appropriate methods are not available to ensure complete destruction of electronic records, the hard drive should be removed to ensure that all traces of personal data are eliminated.

Disposal records

Data controllers should ensure that all relevant contracts of service, MOUs, agreements and written transfer contracts include a retention period for the destruction of personal data after the fulfilment of the specified purpose.⁴⁰ The third party should return the personal data to IOM and certify that all copies of the personal data have been destroyed, including the personal data disclosed to its authorized agents and subcontractors.



Disposal records indicating time and method of destruction, as well as the nature of the records destroyed, should be maintained and attached to project or evaluation reports.

The destruction of large volumes of paper records may be outsourced to specialized companies. In these circumstances, data controllers should ensure that the confidentiality of personal data is guaranteed in writing and that the submission of disposal records and certification of destruction form part of the contractual obligations of third parties.

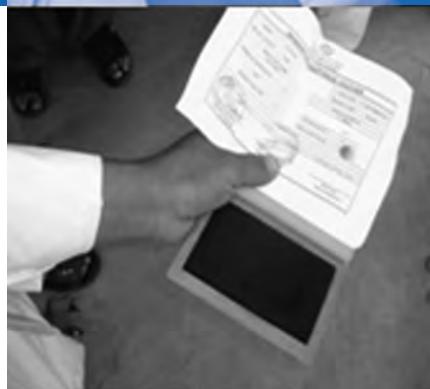
³⁹ Relevant procedures and practices should be followed in coordination with the ITC Department at IOM Headquarters.

⁴⁰ See Template 2.1 outlining a model destruction clause.

10



PRINCIPLE 10: APPLICATION OF THE PRINCIPLES



PRINCIPLE 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.

Personal data should be clearly distinguished from non-personal data because the IOM principles do not extend to non-personal data.

Personal data that have been rendered anonymous in such way that data subjects are no longer identifiable, will continue to fall within the scope of the IOM principles until the personal data collected from data subjects have been effectively eliminated.

Data coding, pseudonymization and anonymization are three common methods of removing identifiable factors in order to preserve the confidentiality of personal data and maintain the anonymity of data subjects.

Box 24: Depersonalizing personal data

- Choose the appropriate method to depersonalize data:
 - data coding;
 - pseudonymization;
 - anonymization.
- Appoint a custodian to secure passwords and key codes.
- To the extent possible, only share anonymous aggregate data with third parties.
- Be confident that anonymity is guaranteed prior to disclosure to third parties.
- Use pseudonyms when reporting case studies and transmitting personal data, especially in the absence of encryption.
- Only publish the identity of data subjects with their explicit consent.

41. Data coding



Data coding is the process of replacing the identity of data subjects, as well as other identifiable factors with labels or unconnected numbers and letters, to preclude identification or render identification substantially difficult to trace.

Data coding involves two steps:

- Dividing the personal data into manageable data sets; and
- Creating and assigning codes to the data sets.

Passwords or keys that decode data sets should be securely stored by data controllers or delegated custodians. Data controllers should ensure that custodians monitor both coded data and personal data stored in computer systems or database applications.

The process of data coding is an effective safety measure and case management tool used for storing and transmitting personal data. It is a useful method for storing personal data in database applications because it allows for effective management of large volumes of personal data and also creates an avenue for separating personal data from non-personal data.



EXAMPLE:

While assigning codes, the categories of personal data could be separated from non-personal data and stored separately within an encrypted database module.

42. Pseudonymization



Pseudonymization is the process of substituting names and using fiction to hide identifying factors and true facts relating to individual data subjects.

To avoid the adverse consequence of identifying data subjects, data controllers should adopt the practice of using pseudonyms for the purpose of reporting case studies and donor reporting.



EXAMPLE:

In the absence of encryption, pseudonyms should be used in the body of e-mails sent to authorized IOM staff.

43. Anonymization



Anonymization is the process of removing all personal identifiers and codes in such a way that there is no reasonable likelihood that data subjects could be identified or traced.

Personal data should be rendered anonymous in such a way that it can no longer, or only with a disproportional amount of skill, time and labour, be attributed to an individual data subject.

Data controllers should always consider sophisticated methods that could be used to trace data subjects before disclosing anonymous data to third parties or making it available for publication (see the introductory part explaining sophisticated methods).

Operational statistical purpose

Anonymous aggregate data may be used for statistical analysis, evaluation, reporting, project management purposes and implementation of related services that benefit data subjects. Written statistical reports or consolidated statistical reports produced by database applications may be disseminated within IOM.

In the absence of consent, only anonymous aggregate data that cannot be used to identify or trace data subjects should be published and disseminated to the public.

When disseminating anonymous aggregate data to third parties, data controllers should take due care, exercise good judgement and take reasonable steps to ensure that there are no traces of personal data in the data set.



EXAMPLE:

The anonymous statistical data set of a medical case study involving 15 women between 30 and 40 years of age, in a remote rural community with a population of 60 women, could be deciphered to reveal the identities of the 15 women.



The primary consideration is whether there is a reasonable likelihood that the data subject could be traced through careful analysis of the anonymous aggregate data set.

Data controllers should ensure that the disclosure of anonymous aggregate data to third parties are governed by a written contractual obligation because, with sufficient amount of determination, anonymous data may be deciphered to identify and trace data subjects.



44. Migration data



Migration data is a compilation of various aggregate data sets that are kept for historical and statistical purposes within IOM.

Migration data are statistical in nature and are gathered from various IOM projects to develop expertise in the area of migration. The use of migration data to map migration trends do not fall within the scope of the IOM principles insofar as it does not rely on or use personal data relating to data subjects.

Migration data that can be used to identify the travel route or link migration movements to an individual data subject will fall within the scope of the IOM principles.

45. Publication

The identities of data subjects and all identifiable factors should be removed prior to publication, particularly with regard to highly sensitive cases and vulnerable data subjects such as trafficked persons.

Unless data subjects explicitly agree to publication, their personal data and images should not be displayed material that is publicly available or information sharing materials such as project updates and reports, newsletters, case summaries and press releases.

In the absence of consent, data subjects should, at a minimum, be informed that their images will be displayed prior to such publication (see also Principle 4).

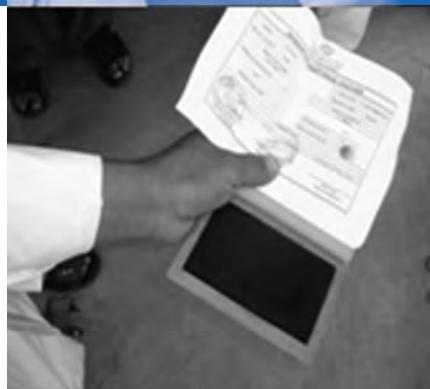
EXAMPLE:

If feasible, only cumulative data sets, and not case-specific details and personal data, should be included in donor reports. The nature of the IOM activity and donor requirements may, however, require full disclosure of personal data. In these circumstances, data subjects should be made aware of such disclosure at the time of data collection and their explicit consent should be obtained.



11

PRINCIPLE 11: OWNERSHIP OF PERSONAL DATA



PRINCIPLE 11: OWNERSHIP OF PERSONAL DATA

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

The assumption of ownership as an institutional standard will allow IOM to maintain ownership of personal data in the event of ambiguities or silence in contracts with third parties. It will also add to the Organization's institutional memory and nurture IOM's unique migration mandate.

46. Ownership clauses

In the absence of donor requirements and written contractual obligation to hand over personal data, data controllers should assert and incorporate an ownership clause⁴¹ into donor contracts, contracts of service, MOUs and sub-agreements.

Written contracts with agents (service providers/consultants), implementing partners, and other third parties should include ownership and destruction clauses. It should also clearly specify that personal data collected on behalf of IOM should be returned to IOM, upon expiration or termination of the contract.

Relationships with IOM partners and implementing partners may involve the collection of different categories of personal data from the same data subjects. In these circumstances, the third party may own the personal data disclosed to IOM. Data controllers should, however, ensure that IOM reserves ownership of subsequent categories of personal data collected by IOM or collected on its behalf.

All existing written contracts that are silent on ownership issues should, to the extent possible, be supplemented by sub-agreements asserting and clarifying the ownership of personal data.



It is within IOM's interest to retain the ownership of personal data collected from data subjects in the course of IOM activities.

Box 25: Ownership considerations

- Clarify ownership in the event of ambiguity.
- Assert ownership in writing.
- Supplement existing contracts with sub-agreements if ownership is not covered in original agreements.
- Where appropriate, ensure that all written contracts with third parties include ownership and destruction clauses, and that personal data is returned to IOM or destroyed upon fulfilment of the specified purposes.



EXAMPLE:

Contracts with research consultants should specify that: IOM reserves all rights of ownership; personal data should be returned to IOM after fulfilment of the terms of the contract; and certification should be provided for the destruction of all copies of personal data.



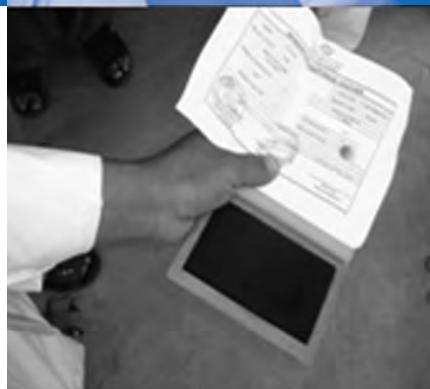
EXAMPLE:

As an IOM partner, the United Nations High Commissioner for Refugees (UNHCR) may disclose personal data to IOM for assistance in the facilitated movement of refugees. If IOM subsequently collects medical data from the refugees, the ownership of the medical data should rest with IOM. Data controllers should ensure that ownership is reserved and secured in writing.

⁴¹ See Template 2.1 outlining a model ownership clause that should be included in all MOUs and agreements, including contracts with implementing partners, IOM partners, donors, service providers, consultants and other third parties.

12

PRINCIPLE 12: OVERSIGHT, COMPLIANCE AND INTERNAL REMEDIES



PRINCIPLE 12: OVERSIGHT, COMPLIANCE AND INTERNAL REMEDIES

An independent body should be appointed to oversee the 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.

Data controllers should encourage training and promote regular reporting to monitor the implementation of the IOM principles.

47. Data protection training

Data protection training should be conducted at all stages of the data processing cycle, from project development and implementation to evaluation and reporting.



Training is a vital tool that should be used to introduce a “culture of data protection” throughout IOM.

Data protection should be filtered into existing training sessions and project proposals should include sufficient costs for independent training sessions, if necessary. Trainers should circulate comprehensive questionnaires at training sessions to map data protection practices at the relevant IOM Field Offices. Interviewers and others involved in the data collection process, as well as new IOM staff and all individuals authorized to handle personal data, should receive orientation on procedures to follow for best practice and compliance with the IOM principles.

It may be useful to arrange joint training sessions with agents (service providers/consultants), implementing partners, IOM partners, donors and government authorities of countries of operation and host countries. This will serve to raise awareness and promote cooperation for the effective implementation of the IOM principles.

Training that falls within the framework of relevant IOM service areas should include data protection safeguards to protect the personal data of training participants. If participant lists are needed for donor reporting or if it is necessary to disclose participant names and contact details in training reports and publications, the data subjects should be informed of such as well as the intended and foreseen purpose(s); consent should be obtained at the time of collecting and signing attendance records.

97

48. Compliance



Chiefs of Missions/Heads of Office and project endorsers or designated IOM staff at the relevant IOM unit/department or regional office should review all project proposals to ensure that data protection is adequately reflected in project development strategies, project activities and budgets.

The necessary costs associated with data protection include, inter alia:

- data security measures;
- hardware and/or software devices;
- staff capacity; and
- training sessions.

Effective compliance indicators include:

- ✓ Advocating awareness and implementing continuous training;
- ✓ Circulating comprehensive questionnaires to map data processing practices at the various IOM Field Offices;⁴²
- ✓ Conducting routine internal audits by circulating checklists at periodic intervals;
- ✓ Submitting assessment reports for annual data protection audits;
- ✓ Ensuring that data protection is included in project development strategies and project proposals under IOM policy considerations;
- ✓ Budgeting for essential costs needed for the implementation of the IOM principles;
- ✓ Including reference to data protection practices in internal/external project evaluation, as well as regular project progress reports required through established IOM reporting channels.

Box 26: Compliance and oversight considerations

- Encourage cooperation among all IOM staff and authorized third parties.
- Raise awareness and liaise with donors and IOM partners and explain that the IOM Principles apply to all projects and is mandatory for all IOM missions..
- Appoint data protection focal points.
- Conduct regular assessments by circulating checklists.
- Provide regular reports through established IOM reporting channels.
- Refer to data protection in project reports and evaluations.
- Welcome annual audits and report complaints and suspicious data protection practices.

Note: Always seek advice from the relevant IOM unit/department, LEG, and the ITC department at Headquarters to ensure compliance with the IOM principles.

The frequency of project reports and evaluation may vary depending on the length of the IOM project and donor requirements. Assessment reports produced for internal project auditing purposes should only reveal non-personal aggregate data and should include, inter alia, a survey of security measures employed and an evaluation of data protection practices.

49. Oversight

Data protection focal points

Regional representatives should ensure that data protection focal points (“focal points”) are appointed to assist with monitoring the implementation of the IOM principles.

The appointment of one focal point per region should be sufficient, unless the size of the region or the number of regional projects handling personal data require multiple focal points. The designated focal point may delegate some of his/her duties to authorized sub-focal points depending on the number of IOM projects handling personal data.

The duties of the focal points may include:

⁴² This will also create the opportunity to approve and oversee the destruction of obsolete electronic and paper records.

- ✓ Familiarity with data protection requirements;
- ✓ Monitoring data protection practices in the relevant IOM region;
- ✓ Promoting the IOM principles and analysing training needs;
- ✓ Collecting assessment reports from data controllers for the purpose of data protection audits;
- ✓ Recommending opinions based on country situations and experience in the region;
- ✓ Assisting with review of project proposals to the extent that it includes data protection;
- ✓ Coordinating with LEG on the application of the IOM principles, particularly in complex cases.

Focal points may assume advisory roles to expedite decisions on data protection issues and bridge the gap between Headquarters and IOM Field Offices, particularly in matters that require urgent attention. LEG and the relevant IOM unit/department should provide support to focal points, as needed.

Data protection audits

To ensure that the IOM principles are adhered to throughout the Organization, data protection should be included as a standard area of review in annual audits. The auditing body responsible for conducting annual audits should be independent and impartial.

The responsibility of the auditing body includes, inter alia:

- ✓ Systematically checking adherence to the IOM principles;
- ✓ Investigating any serious breach;
- ✓ Evaluating the effectiveness of data processing practices.

All data assessment reports and complaints that warrant investigation should be submitted to the auditing body prior to the auditing date. The intensity of data protection audits should be relative to the nature of the personal data processed, the technology used to ensure data security, the consequences of inappropriate data processing practices and the costs associated with conducting annual audits.

50. Internal remedies



Non-compliance with the IOM principles and unlawful data processing should be immediately reported to the data controller, who should investigate complaints without undue delay.

If a complaint is found to be justified, appropriate measures should be taken, including suggestions and recommendations for amending policies and practices.

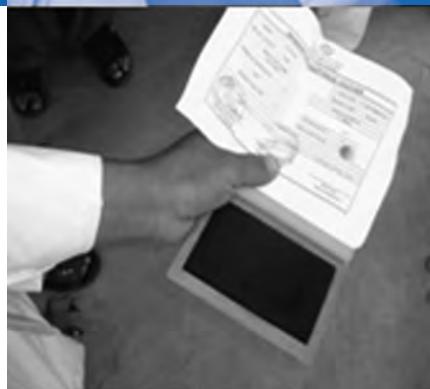
99

Any significant or serious breach of the rights and interests of the data subject that result in harm to data subjects or IOM staff and authorized third parties should be referred to LEG and the Office of the Inspector General at Headquarters. IOM staff involved in any serious breach may be subject to disciplinary procedures.

13



PRINCIPLE 13: EXCEPTIONS



PRINCIPLE 13: EXCEPTIONS

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

All exceptional cases that require derogation from the IOM principles should always be referred to LEG and the relevant IOM unit/department for approval. If the derogation requires the consent of the data subject, data controllers should, to the extent possible, obtain consent prior to the derogation.

51. Intent to derogate

Exceptions to the IOM principles should only be considered if the risks to the privacy of data subjects and the confidentiality of personal data are relatively small and there are competing interests that override the rights and interests of data subjects. Competing interests may include factors such as, *inter alia*, public interest considerations and imminent threats to the life, health and safety of data subjects, as well as of IOM staff and authorized third parties.



Data controllers should engage in a risk–benefit assessment, in coordination with the relevant IOM unit/department, to determine whether the derogation is reasonable and justifiable.

The risk–benefit assessment should be based on reasonableness and proportionality. The benefit to the data subject should be the paramount consideration and all prevailing circumstances should be taken into account.

The limitation on the rights and interests of the data subject should always be proportional to, or appropriately balanced with, any benefits gained from the derogation.

Factors to consider for reasonable justification include the following:

- ✓ nature of the personal data;
- ✓ prevailing circumstances;
- ✓ pressing need to derogate from the IOM principles;
- ✓ purpose achieved by the derogation;
- ✓ nature and extent of the derogation;
- ✓ relationship between the derogation and the specified purposes of data collection and data processing;

103

- ✓ proportionality between the extent of the derogation and the purpose of the derogation;
- ✓ minimal impairment of data protection and the rights and interests of data subjects.



Alternative measures should be considered prior to the approval of the derogation.

The decision to derogate must be fair and should be sufficiently justified because arbitrary decisions will conflict with the purpose of the IOM principles.

52. Conclusion

When handling personal data, data controllers could use a data protection checklist⁴³ to monitor data processing practices in accordance with the data protection measures outlined in these guidelines. The data protection checklist should be signed by the project manager and should be safely stored with the electronic or paper records for oversight, evaluation and reporting purposes.

⁴³ See Checklist 3 outlining a model data protection checklist.

ANNEXURE A

INTERNATIONAL INSTRUMENTS

PRIVACY RIGHTS		
1948	Universal Declaration of Human Rights	Articles 7, 12, 13.
1950	The European Convention for the Protection of Human Rights and Fundamental Freedoms	Article 8
1969	American Convention on Human Rights	Article 11
1966	Covenant on Economic, Social and Cultural Rights	
1966	Covenant on Civil and Political Rights	Articles 12, 17, 26.
1988	United Nations Human Rights Committee, CCPR General Comment No 16: Article 17 (Right to Privacy).	Article17
1989	Convention on the Rights of the Child	Articles 2, 12, 16.
1990	International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families	Articles 1, 8, 14.
DATA PROTECTION		
1980	Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data	
1981	Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as amended with Additional Protocol	
1990	United Nations Guidelines for the Regulation of Computerized Personal Data Files	
1995	European Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.	
2000	Charter of Fundamental Rights of the European Union (Article 8: Protection of personal data)	
2000	Regulation (EC) No. 45/2001 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of such data	
2001	Commission Decision on Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC	



2002	Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks
2005	Committee on the Rights of the Child, General Comment No.6 (2005) Treatment of Unaccompanied and Separated Children Outside their Country of Origin
2006	European Directive 2006/24/EC on the Retention of Data generated or processed in connection with the provision publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
2007	Paris Principles and Guidelines on Children Associated With Arms or Armed Groups
2010	Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

*** Note:** The European Directive 95/46/EC is the most comprehensive instrument on data protection. It is currently under review to: strengthen individuals' rights; enhance the internal market dimension of data protection; revise the data protection rules in the area of police and judicial cooperation in criminal matters; address the global dimension of data protection; and provide a stronger institutional arrangement for better enforcement of data protection rules. For further details, see: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union COM (2010) 609 final, available at: <http://register.consilium.europa.eu/pdf/en/10/st15/st15949.en10.pdf>.

ANNEXURE B

NATIONAL DATA PROTECTION LEGISLATION

- Albania:** Law on the Protection of Personal Data No.9887of 2008
- Argentina:** Personal Data Protection Act No. 25.326 of 2000
- Armenia:** Law of the Republic of Armenia on Personal Data of 2002
- Australia:** Privacy Act of 1988 as amended by the Privacy Amendment (Private Sector) Act 2000
- Austria:** Data Protection Act of 2000
- Bahamas:** Data Protection (Privacy of Personal Information Act of 2003
- Belgium:** Belgian Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the Law of 11 December 1998 implementing Directive 95/46/EC
- Bosnia and Herzegovina:** Law on the Protection of Personal Data of 2001
- Brazil:** Habeas Data Law of 1997
- Bulgaria:** Personal Data Protection Act of 2001(with amendments through 2006)
- Canada:** Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000.
- Chile:** Law for the Protection of Private Life (Ley Sobre Protección de la Vida Privada), Law No.19.628 of 1999
- Colombia:** Law 1266 of 2008 (Habeas Data Act)
- Costa Rica:** Law on Individual's Protection against Personal Data Treatment of 2009
- Croatia:** Act on Personal Data Protection of 2003 (as amended in 2006)
- Cyprus:** Processing of Personal Data (Protection of the Individual) Law 138(1) 2001 (as amended in 2003)
- Czech Republic:** Personal Data Protection Act No. 101 of 2000 (Act No.101 of 4 April 2000 on the Protection of Personal Data and on Amendment to Some Related Laws)
- Denmark:** Act on Processing of Personal Data of 2000 (Act no. 429 of 31 May 2000) (as amended through 2007)
- Estonia:** Personal Data Protection Act of 2003
- Finland:** Personal Data Act of 1999 (523/1999) (as amended in 2000)
- France:** Law 2004-801 of 6 August 2004 modifying Law 78-17 of 6 January 1978 relating to the Protection of Data Subjects as Regards the Processing of Personal Data
- Germany:** Federal Data Protection Act of 2001
- Greece:** Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, as amended by Laws 2819/2000 and 2915/2000
- Hungary:** Act LXIII of 1992 on Protection of Personal Data and Disclosure of Data of Public Interest amended by the Parliamentary Act No. XLVIII, of 2003
- Iceland:** Act on the Protection and Processing of Personal Data of 2000 (No. 77/2000)
- Ireland:** Data Protection Act of 1988 (as amended in 2003)
- Israel:** Privacy Protection Act of 1981 (as amended in 1985 and 1996)
- Italy:** Italian Personal Data Protection Code (Legislative Decree no. 196 of 30 June 2003)
- Japan:** Personal Data Protection Act of 2003 (in force from 1 April 2005)
- Korea (Republic of):** Act on Promotion of Information and Communications Network Utilization and Data Protection 2000 (as amended in 2005)
- Latvia:** Personal Data Protection Law of 2000 (as amended in 2002)
- Lithuania:** Law on the Legal Protection of Personal Data of 1996 (as amended in 2008)
- Luxembourg:** Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data
- Malta:** Data Protection Act of 2001 (in force in 2003)
- Mauritius:** Data Protection Act of 2004
- Mexico:** Federal Law on the Protection of Personal Data of 2010
- Moldova (Republic of):** Law No. 17-XVI of 15 February 2007 on the Protection of Personal Data (as amended by Law No. 141-XVI of 2008)

Morocco: Law No. 09-08 Relative to the Protection of Individuals with regards to their Personal Data of 2009

Netherlands: Personal Data Protection Act of 2000 (in force in 2001)

New Zealand: The Privacy Act of 1993

Norway: Personal Data Act of 2000

Pakistan: Electronic Data Protection and Safety Act of 2005

Panama: Law on the Protection of Personal Data of 2002

Paraguay: Regulation for Personal Data of 2000

Peru: Data Protection Law of July 2001 (Law No. 27.489[4]).

Poland: Act on Personal Protection of Data (as amended in 2004)

Portugal: Act on the Protection of Personal Data of 1998 (Law 67/98 of 26 October)

Romania: Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data of 2001

Russian Federation: Federal Law of the Russian Federation of 27 July 2006 No.152-FZ on Personal Data

Senegal: Law No. 2008-12 of January 25, 2008 on the Protection of Personal Data

Serbia: Law Personal Data Protection of 2008

Slovakia: Act No. 428 of 2002 on Personal Data Protection (No.428/2002 Coll.) (as amended in 2005)

Slovenia: Personal Data Protection Act of 1999 (as amended through 2004)

Spain: Organic Law 15/99 of 13 December 1999 on the Protection of Personal Data

Sweden: Personal Data Act of 1998

Switzerland: Federal Law on Data Protection of 1992

The former Yugoslav Republic of Macedonia: Law on Personal Data Protection of 2005

Tunisia: Data Protection Act of 2004 (Law No. 2004-63 of July 27, 2004)

Ukraine: The Law on Data Protection in Automatic Systems of 1994 (as amended in 2004)

United Arab Emirates: Data Protection Law of 2007

United States of America: The Privacy Act of 1974; Health Insurance Portability and Accountability Act (HIPAA) of 1996; HIPAA Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") of 2000 and The Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) of 2002

United Kingdom of Great Britain and Northern Ireland: Data Protection Act of 1998

Uruguay: Law 17838 for the Protection of Personal Data to be Utilized in Commercial Reports and in Habeas Corpus Actions of 2004 (as amended by Data Protection Act no 18.331 (2008))

Note: This list of national data protection legislation is not exhaustive. A number of countries have privacy provisions in the constitution of the country or telecommunications or other laws covering data protection issues. Other countries such as China, Malaysia, South Africa and Thailand are in the process of developing specific data protection laws. Please see also: <http://www.forrester.com/cloudprivacyheatmap>.

GLOSSARY⁴⁴

Agent means any natural or legal person, government or any other entity that is directly authorized to act on behalf of the data controller for the purpose of achieving the original specified purpose(s) for which personal data are collected and processed.

Aggregate data means information, usually summary statistics, which may be compiled from personal data, but are grouped in a manner to preclude the identification of individual cases.

Anonymity means that the personal identity or personally identifiable data relating to a data subject is unknown.

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.

Armed conflict means “all cases of declared war or of any other armed conflict which may arise between two or more...[States], even if the state of war is not recognized by one of them” (*Art. 2, Geneva Conventions I-IV, 1949*). “An armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a state” (*Prosecutor v. Dusko Tadic, No. IT-94-1-AR 72, International Criminal Tribunal for the Former Yugoslavia Appeals Chamber*).

Asylum-seeker means a person who seeks safety from persecution or serious harm in a country other than his or her own and awaits a decision on the application for refugee status under relevant international and national instruments. In case of a negative decision, the person must leave the country and may be expelled, as may any non-national in an irregular or unlawful situation, unless permission to stay is provided on humanitarian or other related grounds.

Auditing body means an independent and impartial body who is not involved in data collection and data protection and who systematically checks adherence to data protection, investigates any breach and evaluates compliance and implementation of the IOM principles.

Beneficiary means any person who receives assistance or benefits from an IOM project.

Biometrics means the study of measurable biological characteristics. “Biometric identifiers” (BIs) are pieces of information that encode a representation of a person’s unique biological make up (e.g. fingerprints, retinal scans or voice scans). Some governments have introduced the use of biometrics as an improved security measure in issuing passports, visas or residence permits.

Blackberry means a wireless handheld device which supports push e-mail, mobile telephone, text messaging, Internet faxing, Web browsing and other wireless information services.

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

Contractual clause means a special clause in a written contract to avoid problematic ambiguities.

Child means an individual below the age of 18 years unless, under the law applicable to the child, majority is attained earlier (*Art. 1, United Nations Convention on the Rights of the Child, 1989*).

⁴⁴ This Glossary draws primarily on the *IOM Glossary on Migration*, 2nd edition (2011), IOM, Geneva, and relevant international and regional instruments on data protection as outlined in Annexure A.

Child-headed household means any household wherein a child has assumed the role of an adult and has taken over as the head of the household.

Conflict-affected population means a group of people who are affected by an armed conflict.

Country of operation means the country in which the IOM project is being implemented.

Close associates means persons who have a close relationship with the data subject and who act in the best interests of the data subject.

Data controller means an IOM staff or an individual who 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 are 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 who 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 he or she is assigned.

Data security means a set of physical and technological measures that safeguard the confidentiality and integrity of personal data and prevent unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

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

Detention means the restriction on freedom of movement, usually through enforced confinement, of an individual by government authorities.

Donor means any person or entity, often a country, which contributes to the funding of an IOM project.

Due diligence means the care that a data controller exercises when considering transfer to third parties to promote the rights and interests of the data subject.

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

Encryption means a software package to ensure the secure electronic transfer of confidential personal data. The text is converted into incomprehensible code that can only be decoded by the use of a key that protects the original format of the text.

EU means the European Union.

110

EUROPOL means the European Union's criminal intelligence agency that supports cross-border coordination between national law enforcement agencies of EU Member States.

Family unity means a family's rights to live together and, as a fundamental unit of a society, to receive respect, protection, assistance and support. This right is not limited to nationals living in their own State and is protected by international law.

Family reunification means the process whereby family members separated through forced or voluntary migration regroup in a country other than the one of their origin.

Gender sensitivity means recognizing differences and inequalities while promoting the interests, needs and priorities of both men and women, as well as girls and boys.

Host country means a country of destination or a third country. In the case of return or repatriation, also the country of origin.

Human rights means those liberties and benefits based on human dignity which, by accepted contemporary values, all human beings should be able to claim “as of right” in the society in which they live. These rights are contained in the *International Bill of Rights*, comprising the *Universal Declaration of Human Rights, 1948*, the *International Covenant on Economic, Social and Cultural Rights*, and the *International Covenant on Civil and Political Rights, 1966* and have been developed by other treaties from this core (e.g. *The Convention on the Protection of All Migrant Workers and Members of Their Families, 1990*).

Implementing partner means any entity that works side by side with IOM in the execution of an IOM project activity.

Inter alia (Latin) means “among other things,” “for example” or “including”. *Inter alia* is used in these guidelines to precede a list of recommendations or examples that serve as a non-exhaustive list of possibilities.

Internally displaced persons (IDPs) means persons or groups of persons who have been forced or obliged to flee or to leave their homes or places of habitual residence, in particular as a result of, or in order to, avoid the effects of armed conflict, situations of generalized violence, violations of human rights, or natural or human-made disasters, and who have not crossed an internationally recognized State border (*Guiding Principles on Internal Displacement, UN Doc E/CN.4/1998/53/Add.2.*).

International instruments means international and regional conventions, declarations and other legal principles and standards protecting individual liberties and benefits.

INTERPOL means the International Criminal Police Organization.

IOM means the International Organization for Migration.

IOM Field means the operational areas outside IOM Headquarters.

IOM Headquarters means IOM offices in Geneva, Switzerland.

IOM Field Office means IOM offices in operational areas outside IOM Headquarters.

IOM partner means any stakeholder that has a pre-existing agreement to work in cooperation and coordination with IOM, including governments, United Nations agencies, international organizations, non-governmental organizations, research institutions, businesses and private companies.

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.

ITC department means the Information, Technology and Communications Department at IOM headquarters.

ITC officer means any information technology and communications officer as referred to in the IOM Information Technology Policies.

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

Law enforcement agency means a national or international agency that has legal authority to enforce or assist with the enforcement of the law, including police, border police, immigration police, customs or any other law enforcement officials.

LEG means the Office of Legal Affairs at IOM Headquarters.

Memorandum of understanding means a legally binding and mutual agreement between IOM and a third party.

MiMOSA (Migrant Management and Operational Services Application) means the software application used by certain IOM offices to store migrant data, track and manage operational activities, compile statistical reports and improve migrant assistance.

Migration means the movement of a person or a group of persons, either across an international border, or within a State. It is a population movement, encompassing any kind of movement of people, whatever its length, composition and causes; it includes the migration of refugees, displaced persons, economic migrants, and persons moving for other purposes, including family reunification.

National legislation means the law governing the jurisdiction of a State.

“Need to know” basis means the case-by-case granting or denying of authorized access to categories of personal data after careful deliberation.

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.

Partial encryption means the process of applying encryption to electronic storage areas, such as folders, files and database applications containing personal data.

Personal data means all information that could be used to identify or harm data subjects; it is any information relating to an identified or identifiable data subject that is recorded by electronic means or on paper.

Public interest means promoting the greater common good, health or well-being of society as a whole or specific populations.

Public interest research means any research that serves the interests of the public and is necessary for the common good, health or well-being of society as a whole or of specific populations.

Refugee means a person who, “owing to a well-founded fear of persecution for reasons of race, religion, nationality, membership of a particular social group or political opinions, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country.” (*Art. I(A)(2), Convention relating to the Status of Refugees. Art. IA(2), 1951 as modified by the 1967 Protocol*).

Relative means any person who belongs to the same family tree and who is related to the data subject by birth, marriage, adoption or cultural and religious beliefs.

Repatriation means the personal right of a refugee, prisoner of war or a civil detainee to return to his or her country of nationality under specific conditions laid down in various international instruments (*Geneva Conventions, 1949 and Protocols, 1977, the Regulations Respecting the Laws and Customs of War on Land, Annexed to the Fourth Hague Convention, 1907*, human rights instruments as well as customary international law).

Resettlement means the relocation and integration of people (refugees, internally displaced persons, etc.) into another geographical area and environment, usually in a third country. In the refugee context, the transfer of refugees from the country in which they have sought refuge to another State that has agreed to admit them. The refugees will usually be granted asylum or some other form of long-term resident rights and, in many cases, will have the opportunity to become naturalized.

Risk–benefit assessment means the process of evaluating the risks and benefits associated with data processing.

Separated children means children who are separated from both parents, or from their previous legal or customary primary caregiver, but not necessarily from other relatives. These may, therefore, include children accompanied by other family members. In the terms of the *Statement of Good Practice, 2004* in the Separated Children in Europe Programme (SCEP), separated children are “children under 18 years of age who are outside their country of origin and separated from both parents or their previous legal/customary primary caregiver.” The SCEP uses the term “separated” rather than the term “unaccompanied” because “while some separated children appear to be ‘accompanied’ when they arrive in Europe, the accompanying adult(s) may not necessarily be able, or suitable, to assume responsibility for their care.”

Service provider means any entity that provides a service to assist in achieving the specified purpose for which personal data are collected and processed.

Social engineering means the use of deceptive techniques to psychologically trick people into revealing personal data or security access codes.

Social engineer means a person who engages in social engineering to gain unauthorized access to personal data.

Sub-agreement means a legally binding and mutual agreement that supplements a memorandum of understanding or a contract.

Target population group means a particular group of people who are the intended beneficiaries of an IOM project.

Technological obsolescence means that the hardware or software of computer systems or their component parts are no longer technically supported by the manufacturer.

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.

Written transfer contract means a legally binding agreement setting out the terms under which personal data will be transferred to third parties.

Unaccompanied minor/child means persons under the age of majority in a country other than that of their nationality who are not accompanied by a parent, guardian, or other adult who, by law or custom, is responsible for them. Unaccompanied children present special challenges for border control officials, because detention and other practices applied to undocumented adult non-nationals may not be appropriate for children.

Victim of human trafficking/trafficked person means any natural person who is subject to trafficking in persons as defined in Article 3(a) of the United Nations Protocol to Prevent, Suppress and Punish trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention against Organized Crime, 2000.

Vulnerable groups means any group or sector of society that is at higher risk of being subjected to discriminatory practices, violence, natural or environmental disasters, or economic hardship, than other groups within the State; any group or sector of society (such as women, children, the elderly, persons with disabilities, indigenous peoples or migrants) that is at higher risk in periods of conflict and crisis.

Vulnerable data subject means any IOM beneficiary who may lack the legal, social, physical or mental capacity to provide consent.

UNICEF means the United Nations Children's Fund

UNHCR means the United Nations High Commissioner for Refugees

Women-headed household means a household headed by a widowed or divorced female.

BIBLIOGRAPHY

Literature

- Anderson, H.
- 2006 The privacy gambit: Toward a game theoretic approach to international data protection. *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 9, p. 1, available at: <http://law.bepress.com/expreso/eps/1056>
- Asia-Pacific Economic Cooperation (APEC)
- 2005 *APEC Privacy Framework*. APEC Secretariat, Singapore, available at: http://publications.apec.org/publication-detail.php?pub_id=390
- Australian Office of the Privacy Commissioner
- 2006 *Privacy Impact Assessment Guide*. Australian Government, Office of the Privacy Commissioner, Revised May 2010, available at: www.privacy.gov.au
- Bargiotas, T. and E. Maganaris
- 2006 Privacy under attack? The surveillance phenomenon in Europe, the legitimacy of workplace monitoring and the Greek paradigm. *European Review of Public Law*. Esperia Publications, London, 18(3): 1037–1082.
- Barquin, R. and C. Northouse
- 2003 *Data Collection and Analysis: Balancing Individual Rights and Societal Benefits*. Computer Ethics Institute, Washington, D.C., available at: http://www7.nationalacademies.org/cnstat/Barquin_Paper.pdf
- Baker, R.
- 2005 Offshore IT outsourcing and the 8th data protection principle – legal and regulatory requirements – with reference to financial services. *International Journal of Law and Information Technology*, 14(1): 1–27.
- Bergkamp, et al.
- 2002 EU data protection policy: The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy. *Computer Law and Security Report*, 18(1).
- Bianchini, G. et al.
- 2005 *Tomorrow is the tomorrow we should have worried about yesterday: a proposal for an Italian law, regulation usage, retention and deletion of geo-referenced and chrono-reference, automatically collected data containing unique user identifiers*. 20th BILETA Conference: Over-commoditized; Over-observed: The New Digital Legal World?
- Booth, S. et al.
- 2004 *What are 'Personal Data'? A study conducted for the UK Information Commissioner*. The University of Sheffield, UK

Bygrame, L.

- 1998 Data protection pursuant to the right to privacy in human rights treaties. *International Journal of Law and Information Technology*, Vol. 6, pp. 247–284.
- 2001 The place of privacy in data protection law. *University of New South Wales Law Journal*.
- 2002a *Data Protection Law: Approaching its Rationale, Logic and Limits*. Kluwer Law International, The Hague, London, New York.
- 2002b The 1995 EC Directive on data protection under official review - feedback so far. *Privacy Law & Policy Reporter*.
- 2004 Privacy protection in a global context – a comparative overview. *Scandinavian Studies in Law*, Vol. 47, pp. 319–348

Campbell, D. and C. Bàn

- 2005 *Legal Issues in the Global Information Society*. Ocean Publications, New York.

Cavoukian, A.

- 2005 The new breed of practical privacy: An evolution. *Jusletter* 3. October 2005.

Clarke, R.

- 2000 *Beyond the OECD Guidelines: Privacy Protection for the 21st Century*, <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>

Cogan, J. K.

- 2007 Cooperation with international tribunals— binding orders directed at states and international organizations. *American Journal of International Law*, Vol. 101, p. 163.

Cope, H. et al.

- 2002 The right to privacy in personal data: The EU prods the US and the controversy continues. *Tulsa Journal of Comparative and International Law*, Vol. 9, p. 391.

Council of Europe

- 2002 *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection*. Council of Europe, The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
- 2010 *Data Protection: Compilation of Council of Europe Texts*. Directorate General of Human Rights and Legal Affairs, Council of Europe, Strasbourg.

Correa, C.

- 2002 Public health and international law: Unfair competition under the trips agreement: Protection of data submitted for the registration of pharmaceuticals. *Chicago Journal of International Law*, Vol. 3, p. 69.

- Danna, A. and O.H. Gandy
 2002 *All that glitters is not gold: Digging beneath the surface of data mining. Journal of Business Ethics*, Vol. 40, pp. 373–386.
- De Borchgrave, A.
 2001 *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. CSIS Press, Washington, D.C.
- Del Villar, R.
 2001 *Regulation of Personal Data Protection and of Reporting Agencies: A Comparison of Selected Countries of Latin America, the United States and European Union Countries*.
- Dmytrenko, O. and A. Nardali
 2005 .NET Passport under the scrutiny of US and EU privacy law: Implications for the future of online authentication. *Journal of Law and Policy for the Information Society*, Vol. 1, p. 619.
- Eisenhauer, M. and J. Jordan
 2005 *Internal Privacy Governance Frameworks*. 2nd Technical Assistance Seminar on Implementation of APEC Privacy Framework: International Implementation Issues, 2005/SOM3/ECSG/SEM/010, Agenda Item: VI.
- Gandy, O.H.
 2003 *Public Opinion Surveys and the Formation of Privacy Policy*. The Society for the Psychological Study of Social Issues.
- Garcia, F.
 2005 Bodil Lindqvist: A Swedish churchgoer's violation of the European Union's data protection directive should be a warning to US legislators. *Fordham Intellectual Property Media and Entertainment Law Journal*, Vol. 15, p. 1205.
- Guadamuz, A.
 2000 Habeas data: The Latin-American response to data protection. *Journal of Information, Law and Technology*, Vol. 2.
- Gromovs, J.
 2008 *A compendium of legal instruments of the European Union and the Council of Europe concerning the use of security features and biometric identifiers in passport and travel documents, residence permits and short-term visas*. European Commission/International Organization for Migration, Minsk.
- Gutwirth, G. et. al.
 2009 *Reinventing Data Protection?* Springer, Science and Business Media B.V., The Netherlands

- Harper, J. and A. Spies
 2006 *A Reasonable Expectation of Privacy? Data Protection in the United States and Germany*. American Institute for Contemporary German Studies - The Johns Hopkins University. AICGS Policy Report No. 22.
- Holvast, J. et al.
 1999 *The Global Encyclopaedia of Data Protection Regulation*. Kluwer, The Hague.
- Hondius, F.
 1983 A decade of international data protection. *Netherlands International Law Review*, 30(2): 103–128.
- Inter-Agency Standing Committee (IASC)
 2006 *Women, Girls, Boys and Men: Different Needs - Equal Opportunities. IASC Gender Handbook in Humanitarian Action*, <http://www.unhcr.org/refworld/docid/46978c842.html>
- International Organization for Migration (IOM)
 2002 *Emergency Operations Manual*. IOM, Geneva.
 2004 *Research Manual*. IOM, Geneva.
 2005a *Biometrics and International Migration Law*. International Migration Law Series, No. 5, IOM, Geneva.
 2005b *Guide to Selected EU Legal and Policy Instruments on Migration*. IOM, Vienna.
 2006 *Guide on Gender Indicators for Project Development*. IOM, Geneva
 2007a *The IOM Handbook on Direct Assistance for Victims of Trafficking*. IOM, Geneva.
 2007b *Registration Survey Analysis. Technology Application in Migration Management*, Working Group Presentation, IOM, Geneva.
 2009 *IOM Data Protection Principles*. Instruction: IN 138, IOM, Geneva.
 2010a *Migration Initiatives*. IOM, Geneva.
 2010b *Assisted Voluntary Return and Reintegration Handbook*. IOM, Geneva.
 2011 *Glossary on Migration 2nd Edition*. International Migration Law Series, No. 25, IOM, Geneva.
- International Chamber of Commerce
 2003 *Privacy Toolkit: An international business guide for policy makers*. International Chamber of Commerce, France, <http://www.iccwbo.org/uploadedFiles/TOOLKIT.pdf>

International Committee of the Red Cross (ICRC)

- 2002 *The Missing: The legal protection of personal data and human remains*, ICRC, Geneva,
http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf

International Criminal Police Organization (Interpol)

- 2004 *Rules on the processing of information for the purposes of international police co-operation*, as amended by Resolution AG-2005-RES-15, 1 January 2006,
<http://www.interpol.int/Public/ICPO/LegalMaterials/officialDocuments/Default.aspx>
- 2010 *Rules relating to the control of information and access to Interpol's files*,
<http://www.interpol.int/Public/ICPO/LegalMaterials/constitution/control/RulesControlInformation.pdf>

International Labour Organization (ILO)

- 1996 The ILO's code of practice on the protection of workers' personal data.
International Labour Review, 135(5).
- 1997 *Protection of Worker's Personal Data* ILO, Geneva,
http://www.ilo.org/wcms5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

InterAction Protection Working Group

- 2004 Data Collection in Humanitarian Response: A guide for incorporating protection.
Interaction Protection Working Group, Washington, D.C.,
<http://protection.unsudanig.org/data/general/InterAction%20-Data%20Collection%20in%20Humanitarian%20Response%20-A%20Guide%20for%20Incorporating%20Protection.pdf>

James, M.

- 1994 *Privacy and Human Rights: An International and Comparative Study, with special reference to developments in information technology*. United Nations Educational, Scientific and Cultural Organization, Dartmouth Publishing Company Limited, England.

Joint United Nations Programme on HIV/AIDS (UNAIDS)

- 2007 *Interim Guidelines on Protecting the Confidentiality and Security of HIV Information*. UNAIDS, Geneva,
http://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf

Kranenborg, H.

- 2008 Access to documents and data protection in the European Union: on the public nature of personal data. *Common Market Law Review*, 45(4): 1079–1114.

Korff, D.

- 2002 *EC Study on Implementation of the Data Protection Directive: Comparative Summary of National Laws*. Human Rights Centre, University of Essex, UK.

- McCullagh, K.
- 2007 Data sensitivity: Proposals for resolving the conundrum. *Journal of International Commercial Law and Technology*, 2(4).
- Michael, J.
- 1994 *Privacy and Human Rights: An International and Comparative Study, with special reference to developments in information technology*. United Nations Educational Scientific and Cultural Organization (UNESCO), Dartmouth Publishing Company Ltd., France and England
- Moshell, R.
- 2005 And then there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. *Texas Tech Law Review*, Vol. 37, p. 357.
- Organisation for Economic Co-operation and Development (OECD)
- 1996 *OECD Guidelines for the Security of Information Systems*. OECD, Paris.
- 2002 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, includes the "Declaration on Transborder Data Flows" and the "Ministerial Declaration on the Protection of Privacy on Global Networks"*. OECD, Paris.
- 2003 *Privacy Online OECD Guidance on Policy and Practice*. OECD, Paris
- Organization for Security and Co-operation in Europe (OSCE)
- 2004 *National Referral Mechanisms: Joining Efforts to Protect the Rights of Trafficked Persons, A Practical Handbook*. Office for Democratic Institutions and Human Rights/Office for Democratic Institutions and Human Rights, Poland, available at: <http://www.osce.org/odihr/13967>
- Papkonstantinou, V.
- 2001 A data protection approach to data matching operations among public bodies. *International Journal of Law and Information Technology*, 9(1): 39.
- Perruchoud, R. and K. Tömölovà
- 2007 *Compendium of International Migration Law Instruments*. T.M.C. Asser, The Hague.
- Rempell, S.
- 2006 Personal data and subject access rights in the European data directive and implementing UK statute: Durant V. Financial Services Authority as a paradigm of data protection nuances and emerging dilemmas. *Florida Journal of International Law*, Vol. 18, p. 807.
- Shaffer, G.
- 2000 Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards. *Yale Journal of International Law*, 25(1): 1–88.

- Simitis, S.
- 1998 From the general rules on data protection to a specific regulation of the use of employee data: Policies and constraints of the European Union. *Comparative Labor Law and Policy Journal*, Vol. 19, p. 351.
- Stanley, P
- 2008 *The Law of Confidentiality: A Restatement*. Hart Publishing, Oxford, England.
- Swire, P. and R. Litan
- 1998 *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*. The Brookings Institute, Washington D.C.
- Tan, D.R.
- 1999 Personal privacy in the information age: comparison of internet data protection regulations in the United States and European Union. *Loyola of Angeles International and Comparative Law Journal*, 21(4): 661–684.
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
- 2005 *The United Nations and Personal Data Protection*. Jusletter 3, available at: <http://www.adatum.ru/downloads/conferences/27th/The%20united%20nations%20and%20personal%20data%20protection.pdf>
- United Nations Children's Fund (UNICEF)
- 2006a *UNICEF Guidelines on the Protection of Child Victims of Trafficking*. UNICEF, New York, http://www.unicef.org/ceecis/0610-Unicef_Victims_Guidelines_en.pdf
- 2006b *Reference Guide on Protecting the Rights of Child Victims of Trafficking in Europe*. UNICEF, Geneva, http://www.unicef.org/ceecis/UNICEF_Child_Trafficking_low.pdf
- United Nations High Commissioner for Refugees (UNHCR)
- 1994 *Refugee Children: Guidelines on Protection and Care*. UNHCR, Geneva, <http://www.unhcr.org/refworld/docid/3ae6b3470.html>
- 2001 *Guidelines on the Sharing of Information on Individual Cases: “Confidentiality Guidelines”*. Department of International Protection, UNHCR, Geneva, <http://www.humanitarianreform.org/humanitarianreform/Portals/1/cluster%20app/roach%20page/clusters%20pages/CCm/IDP%20Key%20Resources/UNHCR%20Confidentiality%20Guidelines.pdf>
- 2005 *Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information*, UNHCR, Geneva, <http://www.unhcr.org/refworld/docid/42b9190e4.html>
- 2008a *UNHCR Guidelines on Determining the Best Interests of the Child*, UNHCR, Geneva, <http://www.unhcr.org/refworld/docid/48480c342.html>
- 2008b *Access Policy, Archives UNHCR*, <http://www.unhcr.org/3b03896a4.html>

2008c Model agreement on the sharing of personal data with governments in the context of hand-over of the refugee status determination process,
<http://www.unhcr.org/refworld/pfdid/4a54bbf9d.pdf>

Van Wasshnova, M.

2008 Data protection conflicts between the United States and the European Union in the war on terror: lessons learned from the existing system of financial information exchange. *Case Western Reserve Journal of International Law*, 39(3): 827–886.

Walden, I.

2002 Anonymising personal data. *International Journal of Law and Information Technology*, Summer 2002, 10(2): 224.

Walden, I and R. Savage

1988 Data protection and privacy laws: should organizations be protected? *International and Comparative Law Quarterly*, 37(2): 337–347.

Wakan, J.

2003 The future of online privacy: a proposal for international legislation. *Loyola of Los Angeles International and Comparative Law Series*, 26(1): 151–179.

Warren, A. et al.

2001 Sources of literature on data protection and human rights. *Journal of Information, Law and Technology*, Vol. 2.

Webb, P.

2003 A comparative analysis of data protection laws in Australia and Germany. *Journal of Information, Law and Technology*, Vol. 2.

Documentary sources

American Convention on Human Rights, 1969 (entry into force 18 July 1978) [1114 U.N.T.S. 123], available at: <http://www.oas.org/juridico/english/treaties/b-32.html>

Charter of Fundamental Rights of the European Union, 2000, [Official Journal C 364, 18/12/2000 P. 0001 – 0022], available at:
[http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218\(01\):EN:NOT](http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):EN:NOT)

Commission Decision on Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC, 2001 of the European Parliament and of the Council (2010/078/EU), available at <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF>

Convention on the Elimination of All Forms of Discrimination against Women, 1979 (entry into force 3 September 1981) [1249 U.N.T.S. 13], available at: <http://www2.ohchr.org/english/law/cedaw.htm>

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Council of Europe (adopted on 28 January 1981) [ETS No. 108, Strasbourg, 28.1.1981], available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, 1999, Council of Europe (adopted on 15 June 1999), available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/108-1.htm>

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] regarding supervisory authorities and transborder data flows [ETS No. 181, Strasbourg, 08.11.01], available at: <http://conventions.coe.int/Treaty/EN/treaties/html/181.htm>

Convention on the Rights of the Child, 1989 (entry into force 2 September 1990) [A/RES/44/25], available at: <http://www2.ohchr.org/english/law/crc.htm>

Committee on the Rights of the Child (CRC), General Comment No. 6 (2005) Treatment of Unaccompanied and Separated Children outside their country of origin, 1 September 2005 [CRC/GC/2005/6], available at: [http://www.unhchr.ch/tbs/doc.nsf/\(symbol\)/CRC.GC.2005.6.En?OpenDocument](http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CRC.GC.2005.6.En?OpenDocument)

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union COM (2010) 609 final, available at: <http://register.consilium.europa.eu/pdf/en/10/st15/st15949.en10.pdf>

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (adopted by the European Parliament and the Council on 24 October 1995) [Official Journal L 281, 23-11-1995, P. 0031 – 0050], available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Directive 2006/24/EC on the Retention of Data generated or processed in connection with the provision publicly available electronic communications services or of public communications networks_and amending Directive 2002/58/EC (adopted by the European Parliament and the Council on 15 March 2006) [Official Journal L 105, 13/04/2006 P. 0054 – 0063], available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>

European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950 (entry into force 3 September 1953)) [78 U.N.T.S. 222], available at: <http://conventions.coe.int/treaty/en/treaties/html/005.htm>

Guidelines Concerning Computerized Personal Data Files, adopted by the UN General Assembly Resolution, 14 December 1990, United Nations [A/RES/45/95], <http://www.un.org/documents/ga/res/45/a45r095.htm>

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990 (entry into force 1 July 2003) [A/RES/45/158], available at: <http://www2.ohchr.org/english/law/cmw.htm>

International Covenant on Civil and Political Rights, 1966 (entry into force 23 March 1976) [99 U.N.T.S 171], available at: <http://www2.ohchr.org/english/law/ccpr.htm>

International Conference of Data Protection and Privacy Commissioners

- 2005a The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities ("Montreux Declaration"), 16 September 2005, available at: http://www.privacydataprotection.co.uk/documents/montreux_declaration.pdf
- 2005b Resolution on the Use of Biometrics in Passports, Identity Cards and Travel Documents, 27th International Conference of Data Protection and Privacy Commissioners, Montreux, 2005, available at: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2005_Montreux/MONTREUX-EN4.pdf
- 2005c Resolution on the Use of Personal Data for Political Communication, Montreux, 2005, available at: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2005_Montreux/MONTREUX-EN3.pdf
- 2009 The Madrid Resolution International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners, 5 November 2009, available at: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted on 23 September 1980, available at: http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1,00&&en-USS_01DBC.html

Organization for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (adopted on 25 July 2002), available at: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention Against Transnational Organized Crime, Annex II, 2000 [G.A. res. A/RES/55/25], (entry into force 25 December 2003), available at: <http://www2.ohchr.org/english/law/protocoltraffic.htm>

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community Institutions and Bodies and on the free movement of such data, European Parliament and Council [Official Journal L 008, 12/01/2001 P. 0001 – 0022], http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf

Universal Declaration of Human Rights, 1948 [G.A. res. 217A (III)], available at: <http://www.un.org/en/documents/udhr/index.shtml>

United Nations Human Rights Committee (HRC), CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, <http://www2.ohchr.org/english/bodies/hrc/comments.htm>

United Nations Children's Fund (UNICEF), The Paris Principles: Principles and Guidelines on Children Associated with Armed Forces or Armed Groups, February 2007, available at: <http://www.unicef.org/emerg/files/ParisPrinciples310107English.pdf>



IOM Data Protection Templates and Checklists

These templates and checklists are generic in nature and should be used as a guide, where appropriate, to ensure practical application of the IOM data protection principles and guidelines. Please note that all written contracts should be referred to the Office of Legal Affairs LEG@iom.int for review and approval.

CONTENTS	
TEMPLATES	
Template 1: Model consent forms	
1.1 Sample authorization for collection of personal data from beneficiaries	
1.2 Sample beneficiary authorization for participation in IOM projects	
1.3 Sample photography authorization	
1.4 Sample media authorization	
Template 2: General contractual clauses to be inserted into contracts	
2.1 Sample clauses for third parties handling personal data	
2.2 Sample clauses for transfer contracts and processing of personal data	
Template 3: General confidentiality form for staff, interns and consultants	
Template 4: Request form for data subjects seeking access to their personal data	
CHECKLISTS	
Checklist 1: Data quality	
Checklist 2: Data security	
Checklist 3: Data protection	

TEMPLATE 1.1

1.1 Sample authorization for collection of personal data from beneficiaries

GENERAL CONSENT FORM

I, [Name of data subject], hereby authorize the International Organization of Migration (hereinafter, "IOM") and any authorized person or entity acting on behalf of IOM to collect, use, disclose and dispose of my personal data and, where applicable, the personal data of my dependants [Name of child/family members] for the following purposes:

PURPOSES Specified and defined prior to data collection	DESCRIPTION To be filled in by data controllers/interviewers	CONSENT	
		YES	NO
(a) Original specified purpose		
(b) Continuum of assistance		
(c) Additional research purpose		
(d) Additional foreseeable purposes		

I agree that my personal data may be disclosed to the following third parties for the above purpose(s):

	NAME OF THIRD PARTY To be filled in by data controllers/interviewers	CONSENT	
		YES	NO
(e) Authorized IOM staff	fill in authorized staff of different IOM projectsif foresee internal flow within IOM.....		
(f) Authorized third partiesfill in all foreseeable third parties.....e.g. donor, project partners, etc.....		

Data subject's declaration of informed consent:

1. I have been informed about the specified and additional purpose(s) for which my personal data will be collected, used and disclosed, as described above.
2. I understand that my personal data may be used and disclosed for secondary purposes that are necessary to achieve the above described specified purpose(s).
3. I understand that I may access and rectify my personal data on request by contacting IOM.
4. I understand that withdrawal of my consent may result in IOM being unable to provide me with a service for my benefit.
5. I declare that the information I have provided is true and correct to the best of my knowledge.

TEMPLATE 1.1

6. I hereby release, discharge and agree to hold harmless IOM, its officers, employees and agents from any liability or damage caused, directly or indirectly, to me, my family or relatives in connection with this authorization by virtue of the use or disclosure of my personal data for the specified purpose(s) as described above.
7. I understand the contents of this informed consent form after:
 - (a) Having read the above clauses: YES/NO
 - (b) The above clauses have been translated or read to me: YES/NO
8. I voluntarily make this declaration and freely consent to the collection and processing of my personal data by IOM.

Signed at (place).....on (date).....

.....
Interpreter's signature

.....
Data subject's signature or mark
(or parent/guardian/proxy)

* NOTE: This sample consent form is for general use when collecting personal data from data subjects. It highlights the necessary elements to ensure that consent is obtained for specified purposes(s), foreseeable purposes and disclosure to third parties. It is only an outline and can be adapted, as necessary, to meet the objectives of the project. If the consent form is converted into an electronic format by uploading it to a database module for storage purposes, the below consent box could be used to accurately record the form of consent obtained.

CONSENT BOX		
Form of consent obtained from the data subject:		
Explicit		Implicit
written	oral	
List of categories of specified purposes consented to:		
1. Original specified purpose:.....		
2. Continuum of assistance:		
3. Additional research/ other specified purposes.....		
4. Disclosure to staff in different IOM projects.....		
5. Transfer to foreseeable third parties.....		



TEMPLATE 1.2

1.2 Sample beneficiary authorization for participation in IOM projects

BENEFICIARY AUTHORIZATION

I, the undersigned, _____, express my informed decision to cooperate with the International Organization for Migration (hereinafter, "IOM") and to participate voluntarily in the IOM project [name of project]. This project aims to [specify objective of project].

I understand that the personal data of myself and my dependants [name of child/family members] are necessary for the provision of [describe IOM assistance]. I have been informed about the specified and additional purpose(s) and hereby authorize IOM and any authorized person or entity acting on behalf of IOM to collect, use, disclose and dispose of the personal data provided in this form. I am aware and agree that the personal data will be shared with and processed by [name of third party e.g. donors, relevant institutions/government entities] to achieve the specified purpose(s).

I hereby release, discharge and agree to hold harmless IOM from any liability or damage caused, directly or indirectly, to me, my child or my family in connection with this authorization. I agree that in the event of personal injury or death during and/or after my participation in the IOM project, neither IOM, nor any other participating agency or government can in any way be held liable or responsible.

I declare that the information I have provided is true and correct to the best of my knowledge. I understand that if I make a false statement in signing this form, the assistance provided by IOM can be terminated at any time.

Signed on [date] at [place]:

Applicant's signature: _____

* NOTE: This sample beneficiary authorization is an example of a consent statement to be used in IOM projects such as assisted voluntary return and reintegration (AVRR) projects. An adapted version can be included in interview, registration and application forms. It should be noted that the authorization required from the beneficiary will vary depending on the nature of the project and the type of IOM activity e.g. trafficked or assumed trafficked persons will be requested to sign set templates such as the IOM screening interview and assistance interview forms.

TEMPLATE 1.3

1.3 Sample photography authorization

PHOTOGRAPHY CONSENT FORM

I, [name of individual or parent / legal guardian] [as applicable], hereby authorize [name of photographer] on behalf of the International Organization of Migration (hereinafter "IOM") to take photographs (hereinafter "photographs") of my child [name of child] / myself [as applicable]:

1. I consent [on behalf of my child and myself] [if applicable] to being photographed by [name of photographer].
2. I agree and understand that the photographs are being taken within the framework of the project [name of project] (hereinafter the "Project"). This Project aims to [specify objective of project].
3. I authorize IOM to use and reproduce the photographs outside the scope of the Project for future use in its work, including to:
 - Increase knowledge and understanding of migration issues.
 - Raise awareness in campaigns, promotional activities, communication strategies and public communications.
 - Document and promote IOM's work.
 - Inform IOM's donors, partners, the media, the general public and others about IOM's programmes and activities.
4. I understand and agree that future use of the photographs may include, but is not limited to, use in publications, promotional material, brochures, reports, articles, presentations, future exhibitions and display on the websites of IOM and other third-party electronic format media outlets.
5. I understand the nature of the photo shoot and the intended use of the photographs and hereby give my permission for the above-mentioned purposes. I also understand that any photographs taken may be shown in a public environment.
6. I acknowledge that IOM is not obliged to use the photographs.
7. I hereby release, discharge and agree to hold harmless IOM from any liability or damage caused, directly or indirectly, to me, my child or my family in connection with this authorization by virtue of the use of any of the photographs for the purpose of the Project or for IOM's future use.
8. I understand and agree that IOM will have the copyrights and any other intellectual property rights relating to the photographs and that IOM can use and publish them, and authorize third parties to use and publish them, without my consent.
9. I acknowledge that [neither my child nor I] will receive any remuneration for the photo shoot or for the use of the photographs and that no payment or further consideration shall be effected.

TEMPLATE 1.3

10. I understand the contents of this consent form, after:

- (a) Having read the above clauses: YES/NO
- (b) The above clauses have been read to me: YES/NO

11. I voluntarily make this declaration and freely consent to my child/myself being photographed by the photographer on the behalf of IOM.

Signed on [date] at [place]:

Signed by:

[Name]
(Signature or mark of individual or
parent/legal guardian)

[Name]
(Signature or mark of the child)
[if applicable]

Interpreter's signature [if applicable]

TEMPLATE 1.4

1.4 Sample media authorization

MEDIA AUTHORIZATION

I, [name of individual or parent/legal guardian] [as applicable], hereby authorize the International Organization for Migration (IOM) and any authorized person or entity acting on behalf of IOM to disclose my personal information and, where applicable, the personal data of my dependants [name of child/family members] to [name of third party] and to allow them to contact me.

1. I understand that [name of third party] has requested to interview and film me [and my dependant– if applicable] in order to produce and publish my audio and video testimonial for the purpose of:

.....
.....
.....

2. The risks and consequences of my participation in the interview and film have been explained to me and I hereby give my permission for the above-mentioned purpose. I understand that the recording of my audio and video testimonial may be shown in a public environment.

3. Unless I agree otherwise in writing, I understand that [name of third party] will ensure that the following conditions are met:

- (a) My name/address will not be mentioned during the interview and my geographical information will be protected.
- (b) My face/voice will be made unrecognizable.
- (c) A copy of the tape of my interview will be given to me after producing the video film.
- (d) IOM and [name of third party] will use the tape of my interview only for the purpose of producing the video film as requested.

4. I have been informed that a written agreement will be signed between myself and [name of third party]. I hereby release, discharge and agree to hold harmless IOM, its officers, employees and agents from any liability or damage caused, directly or indirectly, to me, my family or relatives in connection with this authorization.

5. I understand the contents of this authorization after:

- (a) Having read the above clauses: YES/NO
- (b) The above clauses have been translated or read to me: YES/NO

TEMPLATE 1.4

I voluntarily make this declaration and freely consent to the disclosure of my personal data by IOM.

Signed at (place).....on (date).....

[Name]
(Signature or mark of individual or
parent/legal guardian)

[Name]
(Signature or mark of the child)
[if applicable]

Interpreter's signature [if applicable]

* *NOTE: This sample media authorization can be used to facilitate access to IOM beneficiaries and/or disclosure of personal data following a request from the media. Unless expressed written consent is obtained from the data subject, faces should be blurred and identities should be hidden. This is particularly important for highly sensitive cases and vulnerable individuals who may be at risk. Requests from the media to gain access to data subjects or their personal data should be assessed on case by case basis after determining the level of risk and ensuring that protection issues are covered.*



TEMPLATE 2.1

2.1 Sample clauses for third parties handling personal data

GENERAL CONTRACTUAL CLAUSES FOR THIRD PARTIES HANDLING PERSONAL DATA

Confidentiality of personal data

.....(name of Third Party)..... shall comply with the IOM data protection principles in the event that it collects, receives, uses, transfers or stores any personal data in the performance of this Agreement.(name of Third Party)..... shall retain the personal data it receives from IOM under strict conditions of confidentiality and security and shall not disclose it to any third party without the prior written approval of IOM. Access to the personal data shall be limited on a strictly applied “need to know” basis to authorized employees and agents of(name of Third Party)..... that agree to be bound by the confidentiality obligations under this Agreement. The confidentiality obligation under this clause shall survive the expiration or termination of this Agreement.

[OR]

Standard confidentiality clause

All information including personal information of the beneficiaries which comes into the(name of Third Party)..... possession or knowledge in connection with this Agreement or the project is to be treated as strictly confidential.(name of Third Party)..... shall not communicate such information to any third party without the prior written approval of IOM.(name of Third Party)..... shall comply with the IOM data protection principles in the event that it collects, receives, uses, transfers or stores any personal data in the performance of this Agreement. This obligation shall survive the expiration or termination of this Agreement.

Confidentiality of source of information

..... (name of Law Agency)..... shall ensure that the identity of the data subject (if disclosed) and the role of IOM in the provision of the personal data, shall remain strictly confidential and shall not be disclosed to any third party under any circumstances, without the prior written consent of the data subject and IOM.

Destruction of personal data

In the event of termination or fulfilment of the specified purpose(s) envisaged under this Agreement,(name of Third Party)..... shall cease to access, use or process any of the personal data received from IOM.(name of Third Party)..... shall return the personal data to IOM and destroy all copies within(retention period)..... / (upon expiration or termination of this Agreement) and shall certify that it, its agents and subcontractors have destroyed all traces of the personal data.

TEMPLATE 2.1

Ownership of personal data

IOM reserves all rights of ownership relating to the personal data it receives from data subjects or collected on behalf of IOM, and all copyright and other intellectual property rights arising out of this Agreement shall be vested in IOM.*(name of Third Party)*..... shall not use, publish, refer to or cite the personal data for any reason, other than that envisaged under this Agreement, without the prior written permission of IOM.

[OR]

Standard intellectual property clause

All intellectual property and other proprietary rights including, but not limited to, patents, copyrights, trademarks and ownership of data resulting from the project shall be vested in IOM, including, without any limitation, the rights to use, reproduce, adapt, publish and distribute any item or part thereof.

Termination of the contract

IOM shall reserve the right to terminate this Agreement at any time without prejudice to any claim for damages and interest, should*(name of Third Party)*..... breach its obligations outlined in this Agreement.

[OR]

Standard termination clause

This Agreement may be terminated by [X month's] written notice to the other Party. However, where the*(name of Third Party)*..... is in breach of any of the terms and conditions of this Agreement, IOM may terminate the Agreement with immediate effect.

* *NOTE: The sample contractual clauses should be adapted according to the nature of the particular contract with the third party. It applies to all contracts with service providers, implementing partners, donors, etc. that involve the collection, receipt, use, transfer or storage of personal data relating to IOM beneficiaries.*

TEMPLATE 2.2

2.2 Sample clauses for transfer contracts and processing of personal data

TRANSFER TO THIRD PARTIES

General data protection clause

.....(name of Third Party)..... shall comply with the IOM data protection principles in the event that it collects, receives, uses, transfers or stores any personal data in the performance of this Agreement. This obligation shall survive the expiration or termination of this Agreement.

.....(name of Third Party)..... understands that IOM is bound by a duty of confidentiality in relation to the personal data it receives from data subjects or collected on behalf of IOM. The personal data shall always remain strictly confidential, and shall not be disclosed to third parties, without the prior written consent of the data subject and IOM.

Non-disclosure

.....(name of Third Party)..... shall comply with the IOM data protection principles in the event that it collects, receives, uses, transfers or stores any personal data in the performance of this Agreement.

.....(name of Party)..... shall use the confidential personal data it receives from IOM, exclusively for the specified purpose(s) envisaged under this Agreement, and shall not indirectly or directly disclose, publish or transmit the same to any third party, without the prior written permission of IOM.

General obligations of the third party

.....(name of Third Party)..... shall take all reasonable and necessary precautions to preserve the confidentiality of personal data and the anonymity of data subjects. All personal data shall be collected, used, transferred, stored securely and disposed of in accordance with the IOM data protection principles.

.....(name of Third Party)..... warrants that it shall comply with the data protection safeguards outlined in this Agreement, and shall perform its obligations under this Agreement in such a way as to ensure that its data protection obligations to data subjects are not breached. In particular,(name of Third Party)..... undertakes:

1. To use the personal data it receives from IOM exclusively for the specified purpose(s) of transfer envisaged under this Agreement.
2. To implement appropriate data security measures to preserve the integrity of the personal data and prevent any corruption, loss, damage, unauthorized access and improper disclosure of the same.
3. To maintain strict standards of confidentiality, employ appropriate access control measures and ensure that all transmissions of personal data are encrypted.
4. To take all reasonable steps to ensure that all its employees, agents and subcontractors abide by the confidentiality obligations under this Agreement.

5. To prohibit any processing of the personal data which is not in accordance with the terms of this Agreement.
6. To immediately update, rectify and/or delete the personal data upon instruction from IOM.
7. To inform IOM of any current or future internal regulations, national laws or regulations which may impact on the IOM data protection principles.
8. Not to further process, disclose, publish or transmit the personal data to any third party, without the prior written permission of IOM.
9. To retain the personal data only to the extent, and in such a manner, that is necessary to fulfil the specified purpose(s) of transfer.
10. To destroy the personal data within (*retention period*)..... / (*upon expiration or termination of this Agreement*) from the date of fulfilment of the specified purpose(s) of transfer and to provide IOM with certification that all traces of the personal data have been destroyed.

Specific obligations of agents collecting personal data on behalf of IOM

Where the(*name of Agent*) , pursuant to its obligations under this Agreement, collects and processes personal data on behalf of IOM, it shall:

1. Adhere to the IOM data protection principles, which form an integral part of this Agreement.
[Attach as annexure.]
2. Collect and process the personal data in accordance with the instructions received from IOM.
[This may be specific or general instructions as outlined in this Agreement, or as otherwise notified by IOM during the data processing period.]
3. Process the personal data only to the extent, and in such a manner, that is necessary to fulfil the specified purpose(s) envisaged under this Agreement.
4. Only transfer the personal data to agents or subcontractors, with the prior written permission of IOM, and in accordance with the IOM data protection principles.

[These obligations should be added to the general third-party obligations outlined above if collecting and processing personal data on behalf of IOM]

* *NOTE: The model contractual clauses should be adapted and supplemented according to the nature of the transfer contract and the relationship that IOM has with the third party. The “confidentiality”, “ownership,” “destruction” and “termination” clauses outlined in Template 2.1 should also be included in the transfer contract.*

TEMPLATE 3

3.1 General confidentiality form for staff, interns and consultants

CONFIDENTIALITY AGREEMENT

I hereby acknowledge that in my capacity as a (*fill in as applicable*) I will have access to confidential personal data relating to IOM beneficiaries.

1. I understand that IOM is bound by a duty of confidentiality in relation to the personal data it receives from data subjects. The personal data shall always remain confidential between IOM and the data subject, and shall not be disclosed to third parties, without the prior consent of the data subject.
2. I shall comply with the IOM data protection principles in the event of the collection, receipt, use, transfer or storage or destruction of any personal data in the performance of this confidentiality agreement.
3. I hereby agree to treat all personal data to which I have access with the utmost care and confidentiality.
4. Under this declaration:
 1. I understand and agree to maintain the anonymity of the IOM beneficiaries and the confidentiality of the personal data disclosed to me.
 2. I understand and agree that I shall not disclose any confidential personal data relating to (*IOM Project name and Project Code*), other than for the specific purpose required by my duties, without the permission of the Project Manager and/or Data Controller.
 3. I understand and agree that during or after my employment with IOM, I shall not disclose any confidential personal data relating to (*fill in IOM Project*) to any other person or entity.
 4. I understand and agree that I cannot discuss case specific details with the media unless I request and receive permission from the Project Manager and/or Data Controller regarding the nature, purpose and limits of any communication with the media.
 5. I agree to notify the Project Manager and/or Data Controller of any breach of my obligations or conflict of interest under this confidentiality agreement.
 6. I understand that a willful violation of this confidentiality agreement will result in appropriate action being taken against me by IOM.
 7. I understand and agree that my obligation to comply with this confidentiality agreement shall survive the termination of my employment with IOM.
5. By signing and returning a copy of this confidentiality agreement to the Project Manager and/or Data Controller of (*fill in IOM Project*) or his/her designate, I confirm my understanding and acceptance of the above mentioned clauses and declare that I will comply with the contents of this agreement.

Signed at (place)..... on (date).....

139

.....
Signature

TEMPLATE 4

4. Request form for data subjects seeking access to their personal data

ACCESS REQUEST FORM FOR DATA SUBJECTS

1. Applicant's last name
2. Applicant's first name
3. Date of birth YYYY/MM/DD
4. Registration/claim number (if applicable/known)
5. Address:
.....
.....
.....
Postal code:.....
Telephone number:.....
6. Are you: (a) the data subject? YES / NO
(b) a representative of the data subject with written authority? YES/NO
7. What categories of personal data do you require?
.....
.....
.....
.....
.....

140

Signed at (place)..... on (date).....

.....
Applicant's signature

CHECKLIST 1

DATA QUALITY CHECKLIST

QUALITY	YES	NO
Have interviewers received training about the importance of preserving data quality throughout the data collection process?		
Have collection sites been examined to ensure a safe and secure environment for the provision of personal data?		
Have interviewers promoted IOM's commitment to confidentiality of personal data?		
Has the need for truthful personal data been emphasized and have the consequences of relying on inaccurate personal data been highlighted?		
Have data subjects validated the categories of personal data provided to the interviewer?		
Have the format and medium of electronic records been examined and transferred to compatible media?		
Are electronic records stored in safe media that are protected from security risks and unauthorized access and have regular backup procedures occurred?		
Are paper records stored in safe locations to prevent wear and tear and unauthorized access?		
Are electronic and paper records readable and have they been updated?		
RELEVANCE	YES	NO
Has the quality of the personal data been affected by any inaccuracies?		
Have any significant changes rendered the original record of personal data unnecessary?		
Have data subjects' circumstances changed, and do new factors render the original record obsolete and irrelevant?		
Have old electronic media been referred to the IOM Information Technology and Communications Department for destruction?		
To what extent is the original record still capable of adding value to the objectives of the IOM project, and is it worth continued storage?		
Can the irrelevant and unnecessary personal data be used for statistical or research purposes that are compatible with the specified purpose for which personal data were collected?		
ACCURACY	YES	NO
Has accuracy been checked by interviewers at the time of data collection?		
Has accuracy been checked by authorized IOM staff when converting paper records to electronic records?		
Have updates been accurately recorded in the electronic and/paper records?		
Has accuracy been checked by authorized IOM staff at the time of retrieval and before use?		
Have categories of personal data been checked prior to use and disclosure?		

Date of previous data quality assessment

Signed at (place).....on (date).....

..... Data controller's signature



CHECKLIST 2

DATA SECURITY RISK ASSESSMENT CHECKLIST

REVIEWING CURRENT SYSTEMS	YES	NO
Are all sensitive personal data within your area of responsibility properly classified according to the level of sensitivity applied to it?		
Have you analysed the level of security at workstations according to sensitivity levels, confidentiality, integrity, transmission and access to personal data?		
Have you identified any environmental, technical, or human factors that raise specific security concerns?		
Have all the important or valuable physical measures and technical measures within your area of control been identified?		
Have you determined ways and means of continuing operations and services in the case of loss of personal data?		
Have you coordinated with the relevant ITC officer to ensure that backup procedures have been regularly conducted to preserve electronic records in the event of accidental loss?		
Have you participated in carrying out reliable checks with authorized staff who store highly sensitive personal data on unprotected computer systems?		
Have you evaluated the storage location and safety measures needed to protect paper records?		
Have you evaluated the electronic storage areas and safety measures needed to protect electronic records?		
Have you enquired about the availability of encryption software?		
IDENTIFYING SECURITY RISKS	YES	NO
Have you examined the security threats to the storage location or computer system used to store personal data?		
Have you examined any weaknesses of the storage location and computer systems?		
Have you assessed the consequence of techniques used by determined individuals to gain unauthorized access to security systems?		
Have you analysed the potential consequences and impacts that the security risks may have on the confidentiality, integrity and availability of personal data?		
Have you foreseen how to mitigate the risks given the existing operational, technical and physical security measures that are available?		
Do you foresee any other risk mitigation solutions that could be applied to the specific workstation?		
IDENTIFIED SAFEGUARDS	YES	NO
Have you identified new security measures to address and reduce the level of security risks?		
Have you tested the feasibility of new identified security measures?		
Have you determined the residual likelihood of occurrence of the threat in the event that the identified safeguards are implemented?		

142

Date of previous data security risk assessment

Signed at (place).....on (date).....

.....
Data controller's signature

CHECKLIST 3

DATA PROTECTION CHECKLIST

DOCUMENTS REQUIRED

(See IOM Data Protection Templates)

- Access request form: (if necessary) to give effect to the data subjects right to access his/her personal data.
- Consent form: incorporating notification of the specified purpose, additional specified purposes, continuum of assistance, additional IOM research/other purposes and foreseeable transfers to third parties. If the consent form is converted to an electronic format or uploaded to database modules for storage purposes, the consent box should be accurately recorded. Consent boxes in electronic format should outline the form of consent and the categories of specified purposes for which consent was obtained.
- Media authorization: allowing access to beneficiaries and/or disclosure of their personal data to the media
- Confidentiality form: authorizing IOM staff, interns and consultants to access and process personal data.
- Data quality checklist: assessing relevance and accuracy throughout the life cycle of data processing.
- Data security checklist: assessing technical and physical data security measures employed throughout the life cycle of data processing.
- Interview, registration and application forms: incorporating data protection, confidentiality, consent statement and other relevant clauses into pre-existing forms.
- Transfer contracts: including data protection, specified purposes, confidentiality of personal data (as well as IOM as source if necessary), non-disclosure, data security, data destruction, ownership, privileges and immunity, and other relevant clauses in service agreements, memorandums of understanding and implementing agreements.

EFFECTIVE PRE-DATA COLLECTION INDICATORS

- Balancing interests: providing an appropriate balance between the goals of the IOM project and the rights and interests of data subjects.
- Proportionality: ensuring that any limitation to data protection is proportional to, or appropriately balanced with, any benefits gained from the IOM project.
- Probability and magnitude of harm: considering the likelihood of harm and how it could affect data subjects and IOM staff or other authorized persons involved in the collection process, and ensuring that adequate safeguards are in place to prevent threats and discriminatory practices.
- Flexibility: being sufficiently flexible to take account of the diversity of individuals affected by the IOM project and considering degrees of heightened sensitivity.
- Disseminating information: providing sufficient information to data subjects to ensure that all the benefits of providing personal data and the actual risks of withholding categories of personal data are clearly understood. Pre-existing relationships with donors, IOM partners, implementing partners and service providers should be communicated to data subjects, and consent should be obtained for additional IOM research purposes and all foreseeable transfers to third parties at the time of data collection.
- Minimum standards: ensuring privacy and confidentiality and promoting adequate measures of protection for the continued processing of personal data.
- Transparency and accountability: ensuring adequate notice, availability of access and complaint procedures, and oversight of the data collection process.
- Review after implementation: assessing the risk–benefit ratio and considering whether there are any unanticipated risks that have evolved, and informing data subjects about any additional risks.

EFFECTIVE RISK–BENEFIT INDICATORS



- Identifying whether limitations to privacy and confidentiality are acceptable in light of the reasonable expectations of data subjects.
- Determining whether the IOM project is of sufficient importance to justify any limitations to the rights and interests of data subjects. The importance of the IOM project should be based on IOM's mandate and the prevailing factors surrounding the particular IOM project. The prevailing factors include the protection of data subject, action required by international community, public interest, human rights abuses, natural disasters, etc.
- Determining whether the safety, health and discriminatory risks are reasonable in relation to the benefits and to what extent the risks can be minimized.
- Considering the special circumstances and vulnerabilities of data subjects and promoting sensitivity to gender, age, language, and social, cultural, or religious attitudes of the target population group or individual data subject.
- Ensuring that appropriate safeguards are included in the data collection process to protect the rights and well-being of data subjects who are likely to be vulnerable to coercion or undue influence such as, inter alia, children, detained data subjects, trafficked or assumed trafficked pregnant women, the physically or mentally disabled, and data subjects who are economically or educationally disadvantaged.
- Providing data subjects with an accurate and fair description of the risks and benefits at the time of data collection.
- Reviewing the balance between the risks and benefits at periodic intervals to account for the possibility of a shift in the risk–benefit ratio.
- Foreseeing adequate training of IOM staff and others involved in the data collection process.
- Analysing how the flow of personal data will impact on the rights and interests of data subjects throughout the life cycle of data processing and ensure that data security measures are applied to minimize the risks and maximize the benefits.

EFFECTIVE PURPOSE SPECIFIC INDICATORS

- Considering the degree to which the specified purpose, related purposes and additional purposes were explained to data subjects at the time of data collection.
- Evaluating whether data subjects would reasonably expect their personal data to be used and disclosed for secondary purposes that seek to fulfil the original specified purpose.
- Maintaining a record of disclosures that are necessary to meet the specified purpose.
- Continually examining the use and disclosure of personal data to ensure that it is limited to the original specified purpose.
- Reviewing whether categories of personal data are used or disclosed for incompatible purposes.
- Identifying necessary steps to be taken to redress incompatible and inappropriate use and disclosure of personal data.

EFFECTIVE COMPATIBLE INDICATORS

- The additional specified purpose (e.g. subsequent research for IOM purposes) was foreseen at the time of data collection and the data subject explicitly provided consent for the sharing of personal data between specified IOM projects to meet the additional specified purpose.
- The additional specified purpose is compatible with the original specified purpose for which personal data were collected and processed.
- Consent was provided at the time of data collection for a “continuum of assistance” with the understanding and appreciation that the personal data will be used by specified IOM units/departments for the continued benefit of data subjects during the life cycle of data processing.
- The additional specified purpose is necessary to render further assistance to data subjects and there is no reason to believe that consent would be withheld, if the impracticality of obtaining consent, did not exist.

EFFECTIVE DATA QUALITY INDICATORS

- Examining the surrounding circumstances of data collection to ensure a safe and secure environment and to foster the truthful provision of personal data.

- Taking reasonable steps to verify the accuracy and truthfulness of personal data at the time of data collection.
- Ensuring that interviewers are adequately trained to preserve data quality throughout the data collection process.
- Encouraging the practice of cross-checking prior to capturing personal data and prior-checking before use and disclosure of personal data.
- Reviewing the categories of personal data, mode of storage and potential consequences of reliance on inaccurate personal data.
- Considering the significance of any inaccuracies and whether it is likely to impact on the continued use of personal data.
- Ensuring that electronic records are technologically compatible with the level of technology used at the relevant IOM field office.
- Promoting reliance on original records of accurate personal data because filtering creates more room for error.

EFFECTIVE NOTIFICATION INDICATORS

- Emphasizing the importance of obtaining consent.
- Explaining the nature and categories of personal data needed.
- Outlining the specified and related purposes for which personal data are collected.
- Ensuring that the benefits of data collection and the need for accurate and truthful provision of personal data are clearly explained.
- Highlighting the internal flow of personal data within the particular IOM project and the necessary flow of personal data between various IOM projects.
- Describing the capturing and storing methods used to ensure data security and confidentiality.
- Clearly explaining use and disclosures, all foreseeable transfers and any additional specified purposes that are foreseen at the time of data collection.
- Providing details about IOM's pre-existing relationships with third parties (agents, service providers, implementing partners, donors, IOM partners, countries of operation, host countries, government agencies, law enforcement agencies, etc.) and explaining the necessary foreseeable disclosures.
- Ensuring that the benefits of data collection, data processing, and all foreseeable transfers are explained at the time of data collection.
- Outlining the consequences of withholding consent and explaining the right to withdraw consent at any phase during the life cycle of data processing.
- Reinforcing IOM's commitment to data protection and explaining access and complaint procedures.

EFFECTIVE CONSENT INDICATORS

- Checking whether data subjects have capacity to consent and contacting the relevant IOM unit/department and the Office of Legal Affairs at IOM headquarters for advice on the collection of personal data relating to children and the mentally disabled.
- Considering the form of consent, i.e. expressed, implied or proxy consent, in the context of the particular IOM project. Always obtain written consent, if feasible. If implied consent is obtained, ensure that data subjects have been notified about the specified purposes. If proxy consent is obtained, ensure that all family members are present and if this is impractical, ensure that their personal data are verified as soon as it is possible to do so.
- Providing all details necessary to ensure that data subjects obtain sufficient knowledge to appreciate and understand the consequence of providing consent.
- Encouraging interviewers to highlight the specified and related purposes, as well as all additional specified purposes such as continuum of assistance, additional research within IOM and other foreseen purposes. Consent should be obtained at the time of data collection for all foreseeable disclosures to third parties.
- Where feasible, ensuring that consent forms or consent statements have been signed, and if personal data are captured with electronic on-site methods ensure that a collective consent signing sheet is circulated and that all data subjects provide written signatures.



- Capturing the list of categories of specified purposes for which consent was obtained and ensuring that conversions to electronic format and database applications include consent boxes.

EFFECTIVE TRANSFER INDICATORS

- Seeking advice from the IOM unit/department and the Office of Legal Affairs at headquarters, prior to disclosure.
- Examining the specified purpose of disclosure and considering how it will serve to fulfil the specified purpose of data collection and data processing.
- Ensuring adherence to the IOM data protection principles and considering national data protection laws and regulations that may also apply to third parties.
- Evaluating the country situation and respect for the human rights and safety of data subjects.
- Ensuring a comparable level of data protection and guaranteeing safeguards under written contractual obligation.
- Encouraging the sharing of anonymous aggregate non-personal data.
- Limiting the amount of personal data to that which is necessary to achieve the specified purpose of transfer, and ensuring that the original records containing personal data are maintained.
- Providing data subjects with an adequate description of the personal data to be transferred and the third parties involved.
- Ensuring that the method of disclosure and transmission of personal data are safe and secure.
- Safeguarding secure transmission by ensuring that the highest level of confidentiality is maintained, using encryption tools for transfer where appropriate, and checking that third parties have compatible decryption tools.
- Maintaining a record of all disclosures indicating reasonable justification for disclosure and identifying the category of personal data disclosed.

EFFECTIVE CONFIDENTIALITY INDICATORS

- Promoting a “climate of confidentiality” by ensuring that all IOM staff, consultants, agents and individuals representing authorized third parties are adequately trained to respect the importance of confidentiality of personal data.
- Ensuring that all IOM staff, consultants, agents, and migrants or other beneficiaries assisting in the data collection process, are adequately trained to communicate IOM’s confidentiality commitment to data subjects at the time of data collection.
- Limiting access to certain categories of IOM staff, consultants and individuals representing authorized third parties.
- Applying strict access controls and maintaining an access record of personal data disclosed.
- Managing security of electronic and paper records to prevent unauthorized retrieval.
- Considering whether data subjects would be susceptible to physical attacks or discriminatory treatment as a result of disclosure.
- Encouraging strict adherence to confidentiality by way of written contractual obligation and ensuring that all third parties agree to respect the confidentiality of personal data prior to disclosure.
- Securing all transmissions of personal data, ensuring that correspondence is highlighted as “confidential” and that recipients of e-mails are carefully selected.
- Substituting codes for identifiers when storing and transmitting personal data, particularly when handling categories of highly sensitive personal data.
- Encouraging the strict compliance with confidentiality to avoid unintentional disclosure to individuals seeking to gain unauthorized access to personal data.
- Monitoring the disposal of printed copies and other paper trails containing personal data, including the shredding of printed material containing personal data.



EFFECTIVE RESPONSE TO ACCESS REQUESTS

- Insisting on proof of identification.
- Considering the best interests of data subjects.
- Revealing categories of personal data on a “need to know” basis.
- Disclosing summaries of individual cases and/or providing copies of electronic or paper records, where appropriate.
- Ensuring that representatives are authorized by data subjects.
- Accepting access requests from representatives in writing.
- Recording access requests, the date of request and the categories of personal data revealed.
- Applying caution to inquiries about data subjects.

EFFECTIVE DESTRUCTION INDICATORS

- Evaluating whether the personal data have been used to fulfil the specified purpose(s).
- Examining whether the personal data can be used for additional purposes in accordance with the IOM principles.
- Coordinating with the relevant IOM unit/department at Headquarters to ensure that personal data are not prematurely destroyed.
- Authorizing destruction and employing the most effective method of elimination.
- Conducting a sensitivity assessment and submitting a categorized list of electronic records to the Information Technology and Communications Department.
- Monitoring the outsourcing of destruction activities, ensuring that third parties sign confidentiality forms to protect the personal data until final elimination, and insisting on the submission of disposal records.
- Monitoring destruction until final elimination and attaching disposal records to final project reports or oversight reports.

EFFECTIVE COMPLIANCE INDICATORS

- Advocating awareness and implementing data protection training.
- Circulating comprehensive questionnaires to map data processing activities in the various IOM Field Offices. This will also create the opportunity to approve and oversee the destruction of obsolete electronic and paper records.
- Seeking advice from data protection focal points, the Office of Legal Affairs, relevant IOM units/departments, and the Information Technology and Communications Department at headquarters.
- Conducting routine internal audits by circulating checklists at periodical intervals.
- Submitting assessment reports for annual data protection audits conducted by an independent auditing body.
- Ensuring that data protection is included in project design and that project proposals sufficiently reflect essential costs needed for the implementation of the IOM principles.
- Including reference to data protection practices in internal/external project evaluation and regular project progress reports through established IOM reporting channels.
- Checking donor reports and publications to ensure that it precludes the identification of data subjects and that all identifiable factors have been removed, particularly if the project involves vulnerable individuals and sensitive cases.

147

Signed at (place).....on (date).....

.....
Data controller's signature

.....
Project manager's signature



IOM International Organization for Migration