INSTRUCTION

INTERNATIONAL ORGANIZATION FOR MIGRATION

Document Title: Migration Data Governance Policy

Document Type: Instruction

Character: Compliance with this Instruction is **mandatory**

Control No.: IN/253

Document Owner: Data Cluster Working Group

Status: Active

Date of Entry into Force: 1 May 2017

End Validity Date:

Replaces – *for Archive Replaced by*: N/A

Summary: Data Governance represents the framework used by IOM to manage the organizational structures, policies, fundamentals, and quality that will ensure access to accurate and risk-free migration data and information. It establishes standards, accountabilities, responsibilities, and ensures that migration data and information usage achieves maximum value to IOM while managing the cost and quality of information handling. Data governance enforces the consistent, integrated, and disciplined use of migration data by IOM.

Keywords: Data Governance**,** policies, fundamentals, migration data, responsibilities, accountabilities

Location: https://intranetportal/Pages/ControlNo.aspx?controlNo=IN/00253

Initiated:	ICT/LEG
Coordinated:	LEG/DGO/ ICT/ Data Steering Group
Authorized:	DGO
Distribution:	All Missions Worldwide, All Departments at HQ

IOM • OIM

Instruction IN/253

INTERNATIONAL ORGANIZATION FOR MIGRATION

Migration Data Governance Policy Date: 1 May 2017

Contents

Tables

Figures

BACKGROUND

I. Background

This Migration Data Governance Policy (the Policy) outlines the standards that guide the Organization's Migration Data Governance. Pursuant to IOM's institutional precepts, the migration data governance policy ensures that IOM is principled in having a migration data governance framework for continued accountability, transparency and efficiency regarding migration data usage and sharing. This policy aligns with IOM's Migration Governance Framework (MiGoF) and IOM's Results Based Management (RBM). The Organization has or might developed specific standards[1] for specific areas of migration data that need to be followed in conjunction with this policy.

THIS POLICY IS INTENDED TO ENSURE THAT

1. There is rigorous accountability through which Migration Data Governance is aligned with IOM's Mission and Strategic Focus.
2. There is governance over IOM's data assets, policy and programming.
3. IOM takes into account relevant international standards and best practices.
4. There are appropriate, open and transparent processes (per IOM structures) in place.
5. Migration data is recognised as an asset of the Organization and protected and managed for the benefit of the whole of the Organization.

Proper implementation of this Policy will contribute to IOM having good quality data which will contribute to ensure funding to assist migrants.

The policy is divided into four sections: I. Background: that provides the context, II Fundamentals: that set out the standards for IOM migration data and it's use, III. Migration Data Governance Structure: that set out the roles of IOM staff in migration data governance; IV. Definitions.

[1] On 1 May 2017, the following policies relevant for migration data are in place in IOM: IOM Data Protection Principles IN/138, IOM Guidelines and Regulation on the Disposal of records and documents IN/5, IT Policies and Guidelines IN/123, as amended from time to time.

BACKGROUND

SCOPE

This policy applies to all IOM migration data in any form, including print, electronic, audio visual, and backup and archived migration data. It does not cover inter alia, IOM staff data, financial data or any other data outside migration data.

This policy applies to all people employed or working for IOM worldwide, whether internationally or locally recruited, regardless of the type or duration of the contract, including interns, secondees, consultants and people holding hourly contracts. For this policy, the term "staff member" shall include all such persons.

PROACTIVE, REACTIVE AND ONGOING MIGRATION DATA GOVERNANCE PROCESSES

IOM may supplement this Policy, as needed with documented procedures for, inter alia, the following areas:

1. Managing Change
2. Resolving Issues
3. Specifying Migration Data Quality Requirements
4. Measuring and reporting value in line with the Results Based Management criteria

POLICY REVIEW

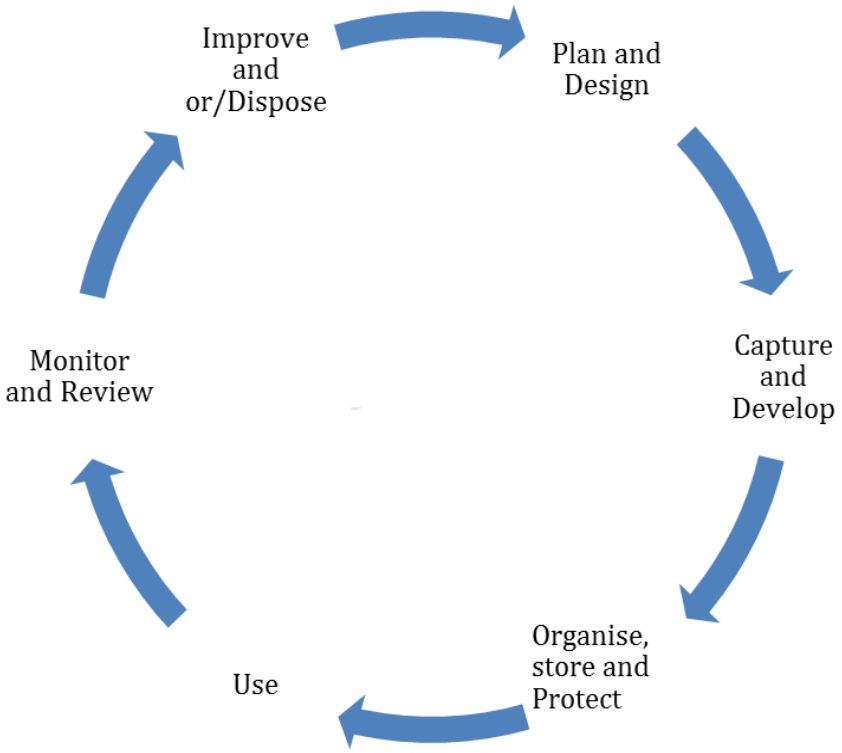
This Policy will be reviewed and updated regularly as appropriate. In this regard the Migration Data Governance Officer shall initiate policy review and ensure that the policy aligns with all IOM policies.

BACKGROUND

MIGRATION DATA MANAGEMENT LIFE CYCLE

The Migration data management life cycle represents the process with which migration data travels until its improvement or disposal.

Figure 1



II. Fundamentals

MIGRATION DATA OWNERSHIP

For all intents and purposes, IOM, the Organization, shall assume ownership of all migration data collected by or on behalf of IOM unless otherwise agreed upon in writing with a third party.

MIGRATION DATA RESPONSIBILITY

Control over specific migration datasets is exercised by Migration Data Stewards who are responsible and accountable for such migration data. Where a migration dataset is relevant to different Migration Data Stakeholders, the Migration Data Steward to whom the specific migration dataset was assigned, needs to consult with the relevant Migration Data Stakeholders (see Responsibility Assignment Matrix 1[2]).

MIGRATION DATA STEWARDSHIP

An individual staff will be assigned as a Migration Data Steward. The Migration Data Steward is accountable for the quality and integrity of a specific migration dataset and for the implementation and enforcement of this Policy and other applicable rules. As of the entry into force of this Policy, a Migration Data Steward must be identified before the collection of the migration data. Any existing migration data must be assigned a Migration Data Steward.

PERSONAL DATA

The IOM Data Protection Principles (IN/138) apply to personal data of IOM beneficiaries and they provide institutional safeguards for handling of such personal data. The collection, use, transfer, storage or any other processing of personal data shall preserve the privacy and dignity of IOM beneficiaries.

[2] Annex 1, Responsibility Assignment Matrix.

FUNDAMENTALS

MIGRATION DATA PROCESSING[3], INCLUDING COLLECTION AND USE

Migration data must not be misused or abused. It must be collected and used ethically and for a legitimate purpose, per applicable international law, the IOM Constitution, IOM's mandate, rules, regulations, standards, and with due consideration for individual privacy. Use of migration data depends on the classification of the migration data (see Migration Data Classification below). Staff must use migration data only to perform IOM's business. The use of IOM migration data (including derived migration data) by staff for personal benefit is prohibited, unless otherwise agreed to be the Organization. Authority to process migration data shall be granted by the appropriate Migration Data Steward only to staff members whose duties specify and require responsibility for migration data update.

MIGRATION DATA SHARING

IOM shares migration data within the framework of its mandate, that is among others, to provide humanitarian aid, to advance the understanding of migration and for improved migration management. Migration data can only be shared for a legitimate purpose and in the best interest of the Organization. In taking a decision to share migration data it must be ensured that the benefit of sharing migration data is balanced against potential risks, considering the level of sensitivity[4] of the data and the imperative to do no harm.

For external Purposes:

Sharing with an external party requires consultation by the Migration Data Steward with other Migration Data Stewards that have a stake in the migration dataset (see Responsibility Assignment Matrix 2, Annex 1)[5]. Where an agreement cannot be reached between the Migration Data Stewards, the approval of the Migration Data Governance Officer should be sought. An agreement, preferably in writing, must be reached with the external party outlining the modalities of the migration data sharing. The agreement must be in line with this Policy and inter alia include that IOM will be recognised and mentioned as the owner of the migration data, unless otherwise agreed by the parties; the migration data is shared for a specified legitimate purpose only; the migration data must not be shared further unless

[3] Processing is used as an overarching term that is used to describe all activities associated with data (cf. MA/88).
[4] See Migration data classification.
[5] Annex 1: Responsibility Assignment Matrix 2.

otherwise agreed between the parties. No migration data sharing agreement is needed for public migration data, unless deemed necessary for the specific instance. To share personal data, IOM's Data Protection Policy (IN/138) need to be followed and LEG must be consulted.

For Internal Purposes:

Migration data can only be shared with the approval of the assigned Migration Data Steward.

If different Migration Data Stewards have a stake in the migration data, due coordination must be done, see the Responsibility Assignment Matrix 2[6]. Due acknowledgement must be given to all involved stakeholder. The migration data governance officer must be consulted where appropriate.

MIGRATION DATA QUALITY

Migration data must be collected at an appropriate quality for the uses to which it is put, or might be put in the future. This shall be achieved by adhering to the data quality principles of accuracy, validity, reliability, timeliness, relevance and completeness. Further standards may be developed by the Organization as needed.

MIGRATION DATA RECORDS

Migration data records must be kept up to date throughout every stage of the migration data life cycle and in an auditable and traceable manner.

MIGRATION DATA CLASSIFICATION

IOM migration data is classified per the risks associated with it and its sensitivity. The related risk assessment must be recorded per Management of Risk in IOM, IN/213. Migration data with the highest risk exposure in case of unauthorized use needs the greatest level; migration data with lower risk requires proportionately less protection. Migration data classification informs the standards for migration data security, including access control, migration data sharing and migration data storage.

[6] Annex 1: Responsibility Assignment Matrix 2.

Table 1: Migration Data Classification

Migration data Category	Description	Risk Exposure in case of unauthorized use
Secret	Highly sensitive information, intended for limited, specific use by individuals with a legitimate need to know. Example: personal data of victims of trafficking.	High risk
Confidential	Sensitive migration data that is internal to IOM that if disclosed could negatively affect operations. Example: Location data of displacement sites in crises that host unaccompanied children.	Moderate risk
Restricted/ Internal Use	Migration data intended for internal IOM business use only. Example: IOM project documents and budgets.	Low risk
Public	Migration data intended for unrestricted use. Migration data can be distributed to the public without restriction. Example: IOM Press Briefing Notes and Publication	No risk

MIGRATION DATA SECURITY

Appropriate migration data security measures must be adhered to always to assure the availability, confidentiality, safety, quality and integrity of IOM migration data. In conjunction with

other applicable IOM organizational standards[7] the following table defines required safeguards for protecting migration data based on their classification.

For the purposes of this Policy, the term "property" includes electronic migration data and migration data warehouses.

[7] On 1 May 2017, the following policies relevant for migration data are in place in IOM: IOM Data Protection Principles IN/138, IOM Guidelines and Regulation on the Disposal of records and documents IN/5, IT Policies and Guidelines IN/123, as amended from time to time.

Table 2: Migration Data Security

DATA SECURITY MEASURES	CLASSIFICATION			
	Secret	**Confidential**	**Restricted / Internal Use**	**Public**
Access Controls	• Viewing and modification restricted to authorised individuals as needed for specific roles. • Migration Data Steward grants permission for access. • Authentication (e.g. password) required for access.	• Viewing and modification restricted to authorised individuals as needed for specific roles • Migration Data Steward grants permission for access, • Authentication (e.g. password) required for access.	• No restriction for viewing • Authorisation by Migration Data Steward required for modification.	• No restrictions
Migration data Retention	• See IN/ 5, IN/123 and IN/138	• See IN/ 5 and IN/123	• See IN/ 5 and IN/123	• See IN/5 and IN/123

Migration data Storage	• See IN/123 • Storage on a secure IOM server required. • Can only be stored on an individual workstation or mobile device if a whole disk encryption is used. • Encryption on back up media required.	• See IN/123 • Storage on a secure server required. • Can only be stored on an individual workstation or mobile device if a whole disk encryption is used	• See IN/123 • Storage on a secure server required.	• See IN/123 • Storage on a secure server required.
Migration data Destruction	• See IN/5, IN/123, IN/88 and IN/138.	• See IN/5, IN /88 and IN/123.	• See IN/5, IN/88 and IN/123.	• See IN/5, IN/88 and IN/123.
Electronic Transmission[8]	• Encryption for data at rest required. • Cannot transmit via email unless encrypted and secured with a	• Encryption for data at rest required.	• Transmission by IOM official email, only	• No restrictions

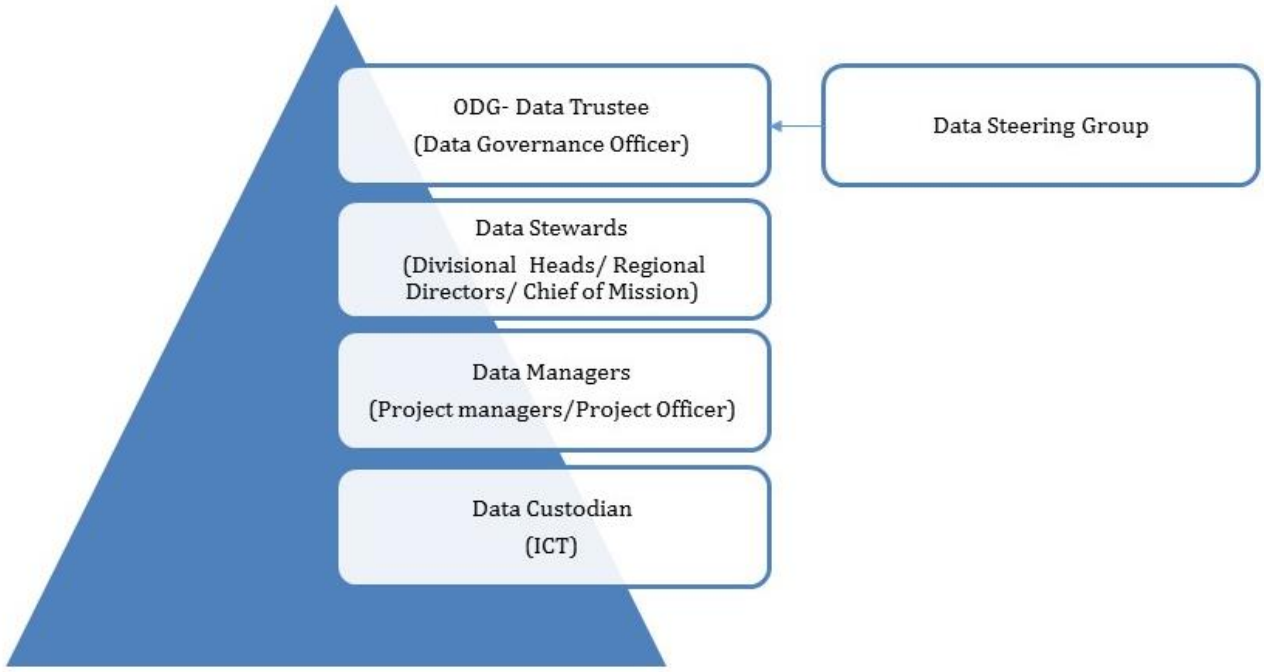
[8] The conditions for sharing migration data are outlined above in this Policy.

	digital signature.			

III. Migration Data Governance Structure

The following graph represents IOM's migration data governance structure.

Figure 2



ROLES AND RESPONSIBILITIES

Migration Data Steering Group

The Migration Data Steering Group has an advisory role to the Data Trustee. The Group was established to support IOM's Migration data governance process and to create cohesion and consistency among the different IOM internal migration data stakeholders. It is composed of migration data stakeholders and their stewards, including departmental and division heads, and representatives from field missions. The Group will convene as needed.

MIGRATION DATA GOVERNANCE STRUCTURE

Migration Data Trustee[9]

Definition: Migration data Trustee means a staff member with oversight responsibility of all migration data. He/she bears responsibility and is accountable for the organization wide migration data strategy, governance, control, policy development, and effective exploitation of migration data.

Roles and Function: The Migration Data Trustee ensures correct processes are followed regarding, inter alia, decision-making, strategy development, resource mobilization, partnerships, use of data so that data assets are managed for the benefit of the organization. As needed, the Migration Data Trustee approves decisions made by the Migration Data Steward(s). Moreover, the Migration Data Trustee oversees initiating the review of this Policy and ensures all relevant requirements, best practices, policies, procedures and any other requirements pertaining to accountabilities of Migration Data Stewards are clearly documented, accessible to all relevant staff and updated as required. The Migration Data Trustee is fulfilling his/her roles and functions considering the interests of all data stakeholders. The Migration Data Trustee fosters coordination and agreement between the Migration Data Stewards. Where agreement cannot be reached, the Migration Data Trustee will take a decision with view to the best interests of the Organization.

Accountability: The Migration Data Trustee is accountable for the organization wide migration data strategy, governance, control, policy development and effective exploitation of migration data.

Title in IOM: For IOM purposes the Migration Data Trustee is the Migration Data Governance Officer.

Migration Data Steward

Definition: Migration Data Steward means a staff member specifically assigned by the Migration Data Trustee in accordance with the Data Governance Policy, accountable for ensuring effective control and use of migration data and information resources in his or her business area.

Roles and Function: The Migration Data Steward ensures that all Migration Data Managers have knowledge and understanding of all relevant legislative requirements, best practices, policies, procedures and any other requirements pertaining to workplace accountabilities of migration

[9] This role is assumed by the Data Cluster Working group chair until the position of the Data Governance Officer has been filled.

data under their stewardship. The Migration Data Steward classifies the migration dataset under his or her responsibility and approves access. Where a migration dataset is relevant to different Migration Data Stakeholders, the Migration Data Steward to whom the specific migration dataset was assigned, needs to consult with the relevant Migration Data Stakeholders (see Responsibility Assignment Matrix 2, Annex 1).

Accountability: The Migration Data Steward is accountable for the quality and integrity of a specific migration dataset and for the implementation and enforcement of this Policy and other applicable rules.

Title in IOM: For IOM purposes each Director of an HQ department or Office, Head of a HQ Division, Regional Director and Chief of Mission is a Migration Data Steward.

Migration Data Manager

Definition: Migration data Manager means a staff member responsible for ensuring effective standard operating procedures and protocols as approved by Migration Data Steward and Trustee and in line with the migration data governance policy are in place to guide the appropriate use of migration data.

Roles and Function: The Migration Data Manager must ensure the process for the administration of migration data is in accordance with the Migration Data Management Life Cycle.

Accountability: The Migration Data Manager is to ensure that all project staff are informed of and have access to documentation regarding all relevant legislative requirements, best practices, policies, procedure and any other requirements pertaining to their project migration data accountabilities.

Title in IOM: For IOM purposes the project manager is the Migration Data Manager.

Migration Data Custodian

Definition: Migration Data Custodian means a staff member who oversees the safe transfer and storage of migration data. They collaborate with the Migration Data Stewards to implement migration data transformations, resolve migration data issues, and collaborate on system changes.

Role and Function: The Migration Data Custodian's focus is on the underlying infrastructure and activities required to keep the migration data intact and available to users. The Migration Data Custodian collaborates with the Migration Data Stewards to implement migration data transformations, resolve migration data issues, and collaborate on system changes.

MIGRATION DATA GOVERNANCE STRUCTURE

Accountability: The Migration Data Custodian is to ensure that they keep informed of all relevant legislative requirements, best practices, policies, procedures and any other requirements pertaining to their work area migration data accountabilities.

Title in IOM: For IOM purposes ICT, will assign a Migration Data Custodian accordingly.

RESPONSIBILITY ASSIGNMENT MATRIX

The following table clarifies the role of Migration Data Steward, Migration Data Manager, Migration Data Custodian and Migration Data Trustee for one migration dataset.

Table 3: Responsibility Assignment Matrix 1
(RACI Table Lower Level)

Decisions Concerning:	Migration data Steward	Migration data Manager	Migration data Custodian	Migration data Trustee Migration data Governance Officer
Migration data standards	A	R	I	Accountable for organizational level migration data and responsible for conflict resolution. Escalation of non-agreement between stakeholders for final decision on such issue.
Migration data Access	A	R	I	
Migration data Collection, Processing and Use	A,	R	I	
Migration data quality	A	R	I	
Migration data classification	A	R	I	
Migration data records	A	R	I	
Migration data security	A	R	I	
Migration data Publishing[10]	A	R	I	
Migration data sharing[11]	A	R	I	
Funding decisions	A	R	I	

[10] Report generation.
[11] Exchange of migration data and /or meta data in a situation involving the use of open, freely available migration data formats, where process patterns are known and standard, and where not limited by privacy and confidential regulations. (DAMA Dictionary)

Liaison	A	R	I		
Migration data Applications	A	C	R		

Responsible, **A**ccountable, **C**onsulted, **I**nformed

IV. Definitions

For the purposes of this Policy:

Access means the process of obtaining or retrieving stored information for use.
Source: Adapted from DAMA dictionary, 2011.

Aggregated migration data means migration data resulting from processes that combine and summarize migration data at the lowest chosen level of detail.
Source: Adapted from DAMA dictionary, 2011.

Confidentiality means a property of migration data indicating the extent to which their unauthorised disclosure could be prejudicial or harmful to the interest of the source or other relevant parties.
Source: Adapted from DAMA dictionary, 2011.

Migration data means any information used to describe and analyse the migration of human beings.

Migration data Governance means the exercise of authority, control, and shared decision making (planning, monitoring, and enforcement) over the management of migration data assets.
Source: Adapted from DAMA dictionary, 2011.

Migration Data Custodian means a person who oversees the safe transfer and storage of migration data. They collaborate with the Migration Data Stewards to implement migration data transformations, resolve migration data issues, and collaborate on system changes.
Source: Adapted from Prime Data Consulting, 2016.

Migration data Life Cycle means a conceptualisation of how migration data is created and used which attempts to define a "birth-to-death" values chain for migration data, including acquisition, storage and maintenance, use, movement to archive, and destruction.
Source: Adapted from DAMA dictionary, 2011.

Migration Data Manager means a person responsible for ensuring effective standard operating procedures and protocols in line with the migration data governance policy are in place to guide the appropriate use of migration data.

Data Protection is the systematic application or 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.
Source: IOM, MA/88.

Migration data Quality means the degree to which migration data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use.
Source: Adapted from DAMA dictionary, 2011.

Migration data Security means a set of physical and technological measures that safeguard the confidentiality and integrity of migration data and prevent unauthorised modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

Source: Adapted from IOM, MA/00088.

Migration data record means a physical grouping of migration data items that are stored in or retrieved from a migration data file. It is referred to as a row or tuple in a relational migration database. A migration data record represents a migration data instance.
Source: Adapted from DAMA dictionary, 2011.

Migration dataset means an organised collection of migration data.
Source: Adapted from DAMA dictionary, 2011.

Migration Data Steward means a person formally and specifically assigned, accountable and responsible for ensuring effective control and use of migration data and information resources in his or her business area.
Source: Adapted from DAMA dictionary, 2011.

Data Subject means any person 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.
Source: IOM, MA/88.

Migration data Stakeholder means any division/ Unit/ Entity that collects, uses or affects migration data in a specific IOM service area.
Source: Adapted from Data Governance Institute, 2016.

Migration Data Trustee means a person with oversight responsibility of all migration data. He/she bears responsibility and is accountable for the organization wide migration data strategy, governance, control, policy development, and effective exploitation.

De-identified Migration data means migration data which has been anonymised and do not identify an individual directly, and which cannot easily be used to determine identity.
Source: Adapted from OECD Health Data Governance, 2015.

Ethical means being in accordance with the rules or standards for right conduct or practice and avoiding conduct that does harm to people.

Operational migration data means process oriented, non-integrated, time current, volatile collections of migration data used to support the daily activities of an enterprise.
Source: Adapted from DAMA dictionary, 2011

Personal data means any information relating to an identifiable data subject that is recorded by electronic means or on paper.
Source: Adapted from IOM, IN/138.

Right to Privacy means "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
Source: UN General Assembly, Universal Declaration of Human Rights, 1948, Article 12. UN General Assembly, International Covenant on Civil and Political Rights, Article 17.1.

DEFINITIONS

Re- Identification means attributing identifying variables to an individual's record within a de-identified migration dataset. Re-identification requires information about the individual obtained from personal knowledge or from migration data stored in other migration datasets about the same individual.
Source: Adapted from OECD Health Data Governance, 2015.

Legitimate purpose means lawful and in line with the organizational standards, instructions and policies.

ANNEX 1: RESPONSIBILITY ASSIGNMENT MATRIX 2

Coordination and Decision Making Processes

The following table clarifies the coordination and decision making process where one dataset is relevant to different data stakeholders. The purpose is to:

1. Align the different data stakeholders with the IOM migration datasets,
2. To increase transparency and collaboration between the stakeholders.
3. To systematically clarify relationships between datasets and to provide clarification on coordination needs between data stakeholders.

Each Migration Data Steward is accountable for his/ her dataset. The table below (Responsibility Assignment Matrix 2) represents how a Migration Data Steward has to coordinate with other stakeholders for which his or her datasets are relevant.

In addition to the table below, where a stakeholder wishes to use the dataset of another stakeholder, the former shall consult with the respective Migration Data Steward. Regional Offices and Missions should always be Informed and Consulted regarding any dataset that belongs to them.

Table 4: Responsibility Assignment Matrix 2
(RACI Table Higher Level)

	GMDAC	MPD	RES	MCD	DTM	RMM	AVM	AVRR	IBM	MHD	LHD	MECC	Regional Offices & Missions
Migration datasets													
Global migration health data (MHD)	C		C		C					R/A/ (Data			C/I

ANNEX 1: RESPONSIBILITY ASSIGNMENT MATRIX 2

	GMDAC	MPD	RES	MCD	DTM	RMM	AVM	AVRR	IBM	MHD	LHD	MECC	Regional Offices & Missions
Migration datasets													
										Steward)			
Global AVM migration data (AVM)	C		C				R/A (Data Steward)						C/I
Global data on resettlement (RMM)	C		C			R/A (Data Steward)				C			C/I
Global data on missing migrants (MCD)	R/C		C	R/A (Data Steward)	I								C/I
Migration Governance data (MPD)	R	R/A (Data Steward)	C	I	I	I	C	C	C	C	C	C	C/I
Global data on migrant return and reintegration (AVRR)	C		C			I		R/A (Data Steward)		C			C/I
Public opinion migration data (GMDAC)	R/A (Data Steward)	C	C	I	C	C	C	C	C	C	C	C	C/I
Migration and Environment data (MECC)	C		C									R/A (Data Steward)	C/I

ANNEX 1: RESPONSIBILITY ASSIGNMENT MATRIX 2

	GMDAC	MPD	RES	MCD	DTM	RMM	AVM	AVRR	IBM	MHD	LHD	MECC	Regional Offices & Missions
Migration datasets													
Irregular migration stocks data methodology (GMDAC)	R/A (Data Steward)	I	C	I	C	I	C	C	C	C	C	C	C/I
Global data on migrant training (LHD)	I										R/A (Data Steward)		C/I
Global data on Displacement (DTM)	C		C		R/A (Data Steward)					C			C/I
Community Engagement Data	I		C	R/A (Data Steward)	C		C	C					C/I

Responsible, **A**ccountable, **C**onsulted, **I**nformed