



MUBADALA



Data Privacy Policy

## Data Privacy Policy

<b>Policy Number: 4.1</b>		
<b>Version Number: 1</b>	<b>Issue Date:</b> 1 May 2017	<b>Effective Date:</b> 1 May 2018
<b>Authorized by:</b>	Mubadala Investment Company PJSC Ethics & Compliance Office  Name: Shahzad Khan  Title: Head of Ethics & Compliance	
<b>Policy Owner</b>	<b>Ethics &amp; Compliance Office</b>  The Policy Owner is responsible for periodically reviewing and updating this Policy so as to reflect regulatory, best practice, and business developments.	

## Applicability & Consequences

This Policy applies to the Mubadala Group and to Mubadala Group Personnel.

Mubadala Group Personnel agree to uphold Mubadala's commitment to do what is right and to follow this Policy and the Mubadala Group Code of Conduct. Mubadala Group Personnel who fail to uphold this commitment put themselves, their colleagues, and the Mubadala Group at risk of fines, penalties, and reputational damage and personally may be subject to disciplinary action, up to and including loss of employment. The Mubadala Group reserves the right, at its sole discretion, to disclose information about violations of law to relevant authorities. Any Mubadala Group Personnel who have violated applicable laws may personally be liable for penalties or fines or be subject to imprisonment.

A Mubadala Group Asset may establish standards that are stricter than this Policy. If a Mubadala Group Asset determines that this Policy is too restrictive for effective business operations, it may submit a written request for deviation, including a detailed justification for the deviation, to the Ethics & Compliance Office.

## Mubadala Group Personnel Responsibilities

### Mubadala Group Personnel are required to:

- Follow applicable laws and regulations;
- Understand and comply with the requirements of this Policy, the Mubadala Group Code of Conduct, other Group Policies, and any Division/Sector or Asset policies or procedures in relation to this Policy;
- Demonstrate ethics, integrity, and accountability at all times and expect the same of those around you; and
- Complete assigned training.

### Leadership will:

- Provide appropriate resources and support to ensure the successful implementation of this Policy; and
- Encourage questions and reporting of concerns and promote corrective actions when needed.

## Help & Reporting Violations

Refer in good faith any questions, concerns, or any known or suspected violations of this Policy to your line manager or other internal management or to the Ethics & Compliance Office (see Appendix 1 for contact information).

Retaliation for good-faith reporting is not tolerated. Mubadala Group Personnel who engage in retaliatory conduct are subject to disciplinary action.

## Definitions

Throughout this Policy, defined terms are capitalized and have the following meanings:

- **Anonymization:** Elimination of all identifying elements from Personal Data; no element may be left that could serve to re-identify the Person. Where information has been successfully anonymized, it is no longer Personal Data.
- **Asset:** Any company or business within the Mubadala Group.
- **Business Partner:** Includes any party (i.e., natural person or legal entity) with which the Mubadala Group conducts business, remits funds to, or receives funds from, including (but not limited to) customers, suppliers, vendors, consultants, advisors, contractors, distributors, agents, partners, and mergers and acquisitions targets.
- **Data Controller:** Individual or company that determines the purposes for which any Personal Data is to be processed.
- **Data Subject:** The Person who is the subject of Personal Data; the Person about whom Personal Data relates.
- **Division/Sector:** A business or corporate function of Mubadala.
- **Ethics & Compliance Office:** The Mubadala Ethics & Compliance Office or relevant Asset ethics & compliance function.
- **Group Policy(ies):** Any policy that applies to the Mubadala Group. Group Policies do not include policies that only apply to a limited set of Mubadala Group Personnel, for example, a policy that only applies to a specific Division/Sector or Asset within the Mubadala Group.
- **Healthcare Facility:** A hospital or healthcare center of the Mubadala Group.
- **Leadership:** The Chief Executive Officer or equivalent of the Mubadala Group, a Mubadala Sector or Division head, or, in each case, a nominated representative.
- **Mubadala Group:** Mubadala Investment Company PJSC (Mubadala); any entity, operation, or investment controlled by Mubadala; and/or any entity, operation, or investment that adopts the Mubadala Group Code of Conduct.
- **Mubadala Group Personnel:** All individuals who work directly for or represent the Mubadala Group, including directors, employees, consultants, and long-term contractors of the Mubadala Group.
- **Person:** Natural person or human being.
- **Personal Data:** Information relating to an identified or identifiable Person. Information may be Personal Data if it may lead to the identity of a Person by obtaining additional information.
- **Processing:** Any operation, whether manual or automated, performed on Personal Data, including but not limited to collecting, recording, organizing, storing, adopting, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, blocking, erasing, or destroying.
- **Pseudonymization:** The process of replacing Personal Data with a pseudonym, for example, replacing a name with an identification number.

- **Sensitive Personal Data:** Personal Data that requires enhanced protection due to the delicate nature of the information. This information includes racial or ethnic origin, nationality/passport, political opinions, religious or similar beliefs, trade union membership, physical and/or mental health information, credit card number, government-issued identification (e.g., driving license, national identification, passport, etc.), and criminal convictions, allegations, court proceedings, and/or sentences.

## Policy Summary

The Mubadala Group is a global company with presence in many industries and territories. Each country and industry may have its own laws and regulations for data protection and Processing. Many of these laws and regulations specifically aim to protect information relating to Persons and restrict accessing Personal Data, sharing Personal Data with other Mubadala Group Assets or with third parties, and/or transferring Personal Data across geographic borders.

This Policy sets minimum expectations to ensure that the Mubadala Group adopts good practices and conducts its business in a compliant manner. Leadership of the Mubadala Group, who bear responsibility for data privacy activities, are obliged to ensure that data protection requirements are in place and met. Internal Audit is responsible for conducting regular data protection audits to ensure compliance with data protection policies and applicable data protection laws. This Policy sets out eight basic principles (listed below) for collecting and Processing Personal Data:

- Fair and Lawful Processing
- Restriction to a Specific Purpose
- Relevance
- Accurate and Up-to-Date
- Technical and Organizational Security
- Data Retention
- Right to Access
- Data Transfer

In many countries, data protection laws protect individuals from abusive Processing, transferring and sharing of Personal Data. Violations of relevant data protection laws and/or employment laws may lead to legal proceedings and claims for damages against the violator (whether the violator is a company, employer, or individual). Local laws take precedence over this Policy, and it is essential to follow applicable local laws.

This Policy is to be used in conjunction with the Mubadala Group Code of Conduct and any other relevant Mubadala Group or local policies.

## Policy Requirements

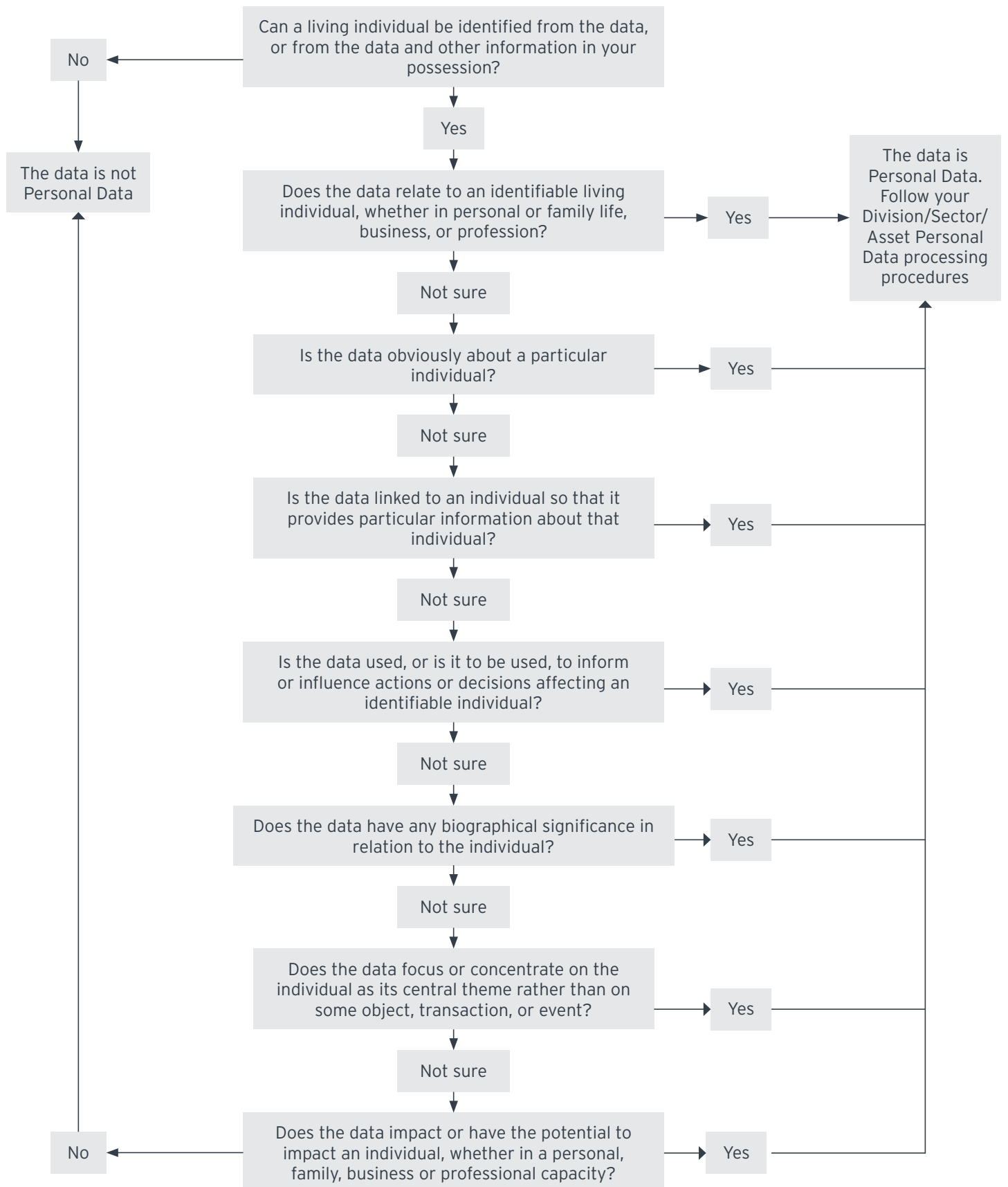
### 1. Personal Data

Personal Data is broadly defined as information that relates to an identified or identifiable Person (i.e., the Data Subject). There are different ways in which a Person may be identifiable. A Person's name is obvious Personal Data. A Person also may be identifiable from other information that may be used to reference another source, such as physical characteristics, social identity number, address, employee ID number, email address, etc.; this is Pseudonymization. Personal Data remains subject to data protection laws even if it is publicly-available, e.g., telephone number, email address, etc.

Under some countries' (e.g., European Union) legislation, some Personal Data is classified as Sensitive Personal Data which is often given more protection. Sensitive Personal Data may include (but is not limited to) race, ethnicity or national origin, political opinions or associations, union membership, marital status, health-related information, and criminal history.

The Mubadala Group bears responsibility for applying appropriate security measures for Personal Data, including Sensitive Personal Data, it acquires from Mubadala Group Personnel, job applicants, Business Partners, and terminated or retired Mubadala Group Personnel.

The flowchart below, illustrates how to determine whether information is Personal Data:



## 2. Principles for processing data

The Mubadala Group controls, possesses, and processes Personal Data on a variety of Persons, including Business Partners. In order to comply with legal requirements and maintain good business standards, the Mubadala Group must process and protect Personal Data in a manner consistent with good practices and applicable law. Where local law is stricter than this Policy, local law prevails.

This Policy adopts eight basic principles of data protection. Local law may permit deviation from a principle under particular circumstances. Consult with the Ethics & Compliance Office prior to deviating from one of the data protection principles of this Policy, even if deviation is permitted by local law.

A Data Controller is responsible for and must be able to demonstrate compliance with each of the following principles:

- i. **Fair and Lawful Processing:** Personal Data is to be processed fairly, transparently (to the Data Subject), and in accordance with law. To create transparency, Data Controllers are to provide concise, accessible, clear, and plain information to Data Subjects including the identity and contact details of the Data Controller, purpose(s) of processing, and data recipients. Local law may require additional information to be included in a privacy notice. A Data Controller may also be required by law to obtain consent from a Data Subject prior to processing Personal Data.
- ii. **Restriction to a Specific Purpose:** Personal Data should be collected only for specified purposes and should not be Processed in a manner incompatible with those purposes. Purposes for Processing data always should be business-related, legitimate, and clear.
- iii. **Relevance:** Personal Data must be adequate, relevant, and not excessive in relation to the purposes for which it is Processed.
- iv. **Accurate and Up-to-Date:** Personal Data should be accurate and updated when necessary. Suitable steps must be taken to ensure that inaccurate or incomplete data is deleted or corrected.
- v. **Technical and Organizational Security:** Appropriate technical and organizational security measures must be taken to prevent unauthorized, unlawful Processing and accidental loss, destruction, or damage to Personal Data. Access to Personal Data must be appropriate for the type and scope of Mubadala Personnel who will have access and on as-needed basis only. The appropriate Mubadala Group information technology function may provide support for securing Personal Data and for Anonymization and Pseudonymization to ensure that data is kept confidential and secure.
- vi. **Data Retention:** Personal Data should not be retained longer than necessary (for example, only the time required to fulfill the purpose for which it was collected). Unnecessary Personal Data must be deleted or disposed of in a secure way that protects the interests of the Data Subject.
- vii. **Right to Access:** Personal Data must be made available to the Data Subject to correct or amend inaccurate Personal Data, and the Data Subject may request deletion of Personal Data that is no longer necessary.



viii. Data Transfer: Personal Data may only be transferred to another party (whether related or unrelated) or third party if there is a legitimate business purpose and the other party has data protection measures comparable to those set out in this Policy or as required by applicable law or regulation. A transfer outside the geographical location should be pre-approved by the Ethics & Compliance Office to ensure the appropriate level of protection and compliance with applicable law.

### **3. Data Processing Legitimacy**

Personal Data may be Processed only for specified, clear, and legitimate purposes. Processing Personal Data is permissible if Processing is:

- Performed with the consent (when required) of or after proper notification (see Appendix 2 - example of notification message) to the Data Subject;
- Necessary for the purpose of establishing a contractual relationship or similar relationship of trust with the Data Subject;
- Necessary to safeguard justified interests of the company;
- Permitted or agreed by applicable local law and regulations;
- Necessary for compliance with legal obligations to which the company is subject; or
- Required to protect the life, health, or safety of the Data Subject.

### **4. Consents**

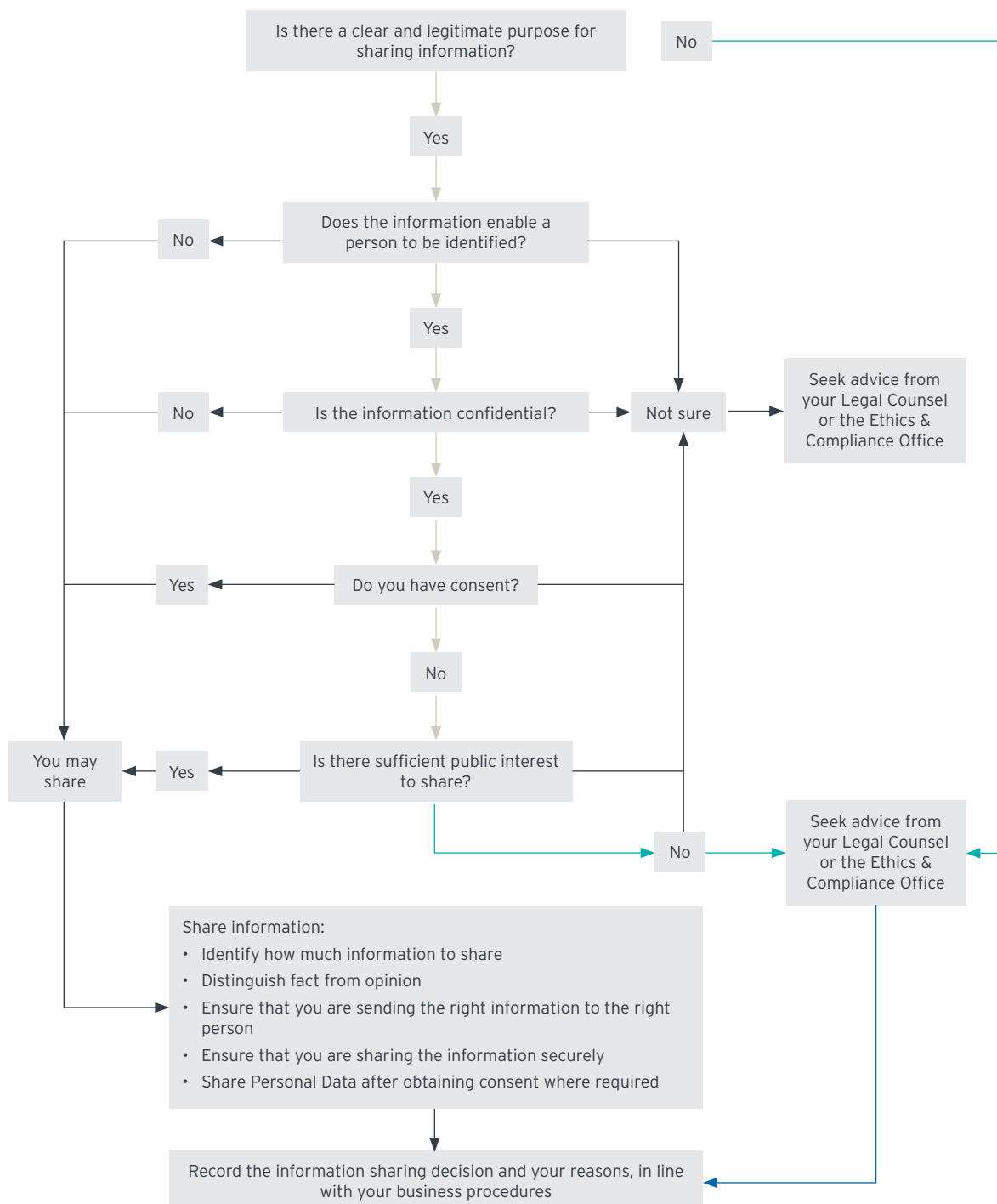
Whenever possible and always where required by law, a Data Subject should give consent before Processing, sharing, or transferring his/her Personal Data. To be effective, consent must be informed, which means that the Data Subject must know and understand why the Personal Data is being processed, shared, or transferred. In addition, consent must be given freely and voluntarily in order to be valid. Consent may be given in written, electronic, or verbal form. Verbal consent should be noted in a record for future reference. Where prior consent is required, the purpose of data Processing may only be changed with the consent of the Data Subject or to the extent permitted by law. In some countries, previously given consent may be withdrawn at any time, and the Data Controller must be able to demonstrate that it has acted on the request.

### **5. The Data Subject's access right and request**

The Mubadala Group will allow Data Subjects reasonable access to Personal Data during normal working hours and upon reasonable request and will allow a Data Subject to update and/or correct inaccurate information. The Data Protection Lead shall establish a method to enable Data Subject rights of access, removal, or rectification where appropriate and in compliance with reasonable policies and procedures.

## 6. Data Sharing

For some business processes, it may be necessary (e.g., legal obligation) or desirable (e.g., practicality) to share Personal Data outside the organization that possesses it. Before sharing or transferring Personal Data, the Mubadala Group should consider if transmitting Personal Data (even if to related entities) is necessary, appropriate, legitimate, and compatible with the purpose(s) for which it was obtained, or is in conflict with any interest of the Data Subject. The recipient must guarantee an adequate level of data protection in line with this Policy and applicable law and be bound by contract to process Personal Data only for specified, legal purposes. The flowchart below sets out the key questions to be considered before information sharing:



## 7. Special Responsibilities

Particular functions, Mubadala Group Personnel, and Business Partners have specific responsibilities to ensure the success of this Policy. These responsibilities are detailed below:

### a. Asset Leadership

- Appoint a Data Protection Lead;
- Support the implementation of the data privacy program, demonstrate commitment to accountability, and implement mechanisms to ensure responsible decision-making about the protection of Personal Data and adoption of internal practices consistent with the law and Mubadala Group Policies;
- Consult with the Ethics & Compliance Office and information security team before establishing or updating any system, process, or procedure to collect, use, disclose, or transmit Personal Data;
- Establish ongoing oversight, monitoring, auditing, and review of privacy and data protection practices to ensure continuing compliance with the law and this Policy;
- Notify the Ethics & Compliance Office of any data breach to comply with relevant data protection regulations and legislation;
- Implement a remediation plan and manage corrective actions in the event of a data breach; and
- Support mechanisms and procedures for individuals to report misuses or inappropriate disclosure of Personal Data and support appropriate remediation and disciplinary actions.

### b. Data Protection Lead (DPL)

Leadership will appoint one person or a team of persons to be its DPL. The DPL need not to be a full-time role or new position within the organization. The business may assess and decide, according to its needs, whether the DPL should be a dedicated responsibility or an additional responsibility of an existing role in the business. The responsibilities of a DPL may include, but are not limited to, the following:

- Identify the Personal Data controlled, requested, acquired, processed, and/or maintained by the business;
- Develop processes and procedures for handling Personal Data that are in compliance with this Policy and local law and are suitable to business needs;
- Communicate internal data protection policies and processes to Mubadala Group Personnel and Business Partners, as appropriate;
- Monitor the proper use of Personal Data Processing, transferring, sharing, and disposing of Personal Data in accordance with applicable data privacy regulations and this Policy;
- Be involved in any Personal Data activities related to Processing or (external) transfer, especially those outside the country;
- Conduct a risk assessment to identify potential data protection risks and put in place a plan to mitigate those risks;
- Alert the business to any risks that might arise with regard to data privacy; and

- Handle data privacy-related queries and complaints and notify the Ethics & Compliance Office of any failure to comply with relevant data protection legislation or this Policy.

### **c. Human Capital**

Human Capital are custodians of much Personal Data within any organization, not limited to employee data, but also potential new candidates' Personal Data. Personal Data collected for recruitment must be limited to the information necessary to evaluate the suitability of a candidate and career potential and to perform any necessary security or other vetting. Mubadala Group Human Capital functions should follow their applicable and relevant processes and procedures before Processing Personal Data.

Human Capital should inform Mubadala Group Personnel and candidates about the purposes for which Personal Data will be Processed, the type of Personal Data stored, the parties with which Personal Data is regularly shared (including government), and the purpose and legal bases of such sharing and Processing (see Appendix 2 - example of notification message). It is sufficient for the purposes of this Policy that Mubadala Group Personnel are informed about Processing and sharing by means of a Human Capital policy (or similar method). Local laws however take precedence over this Policy, and it is essential to follow applicable local laws.

### **d. Healthcare Facilities**

Mubadala Group Healthcare Facilities have access to Sensitive Personal Data in patient medical records. Healthcare Facilities have access to medical data that may be processed for the purposes of preventive medicine, medical diagnoses, providing care, treatment, or managing healthcare devices. Mubadala Group Healthcare Facilities have a legal and ethical obligation to protect patient Sensitive Personal Data and to ensure that it is accessed only for authorized, necessary purposes. To protect Personal Data and Sensitive Personal Data, Anonymization or Pseudonymization is preferred for Personal Data used for scientific or research purposes.

### **e. Third Party Processing**

A Division/Sector or Asset may use an external party to assist and support in Processing activities. The external party must provide necessary security measures and take reasonable steps to ensure compliance with this Policy and applicable laws and regulations. A written contract shall require a third party processor to comply with data privacy and security requirements and will require notification to the appropriate Mubadala Group Division/Sector or Asset if a breach occurs.

Personal Data shall not be transferred to another party, country, or territory, unless reasonable and appropriate steps, including approval when required, have been taken to maintain the required level of data protection.

Subject to written agreement, Personal Data may be communicated to other parties by the third party only for reasons for which the Personal Data was originally collected or other purposes authorized by law.

It is a best practice to use Pseudonymization to transfer Personal Data and Sensitive Personal Data outside the company. Use Anonymization wherever possible.

The Division/Sector or Asset should monitor and conduct checks on Processing Personal Data by any third party, especially in respect of security measures to ensure compliance with this Policy and contractual commitments.

## Appendix 1

### Ethics & Compliance Contact Information

**Global number (Mubadala head office, Abu Dhabi):** +971 2 413 3333

**Toll-free numbers are available for the following countries:**

United Arab Emirates 800 413 3333  
Outside UAE (listed below): 800 2 444 3333\*

Australia	France	Malaysia	South Korea
Austria	Germany	New Zealand	Switzerland
Argentina	Hong Kong	Norway	Taiwan
Belgium	Italy	Philippines	Thailand
Canada	Japan	Singapore	UK
China	Macau	South Africa	USA

\*This toll-free number is only available from the countries listed above. Before dialing the number, you will need to dial your country's international dialing code (e.g., 011 for USA, 00 for UK, etc.) OR dial "+" on your mobile phone.

Facsimile: +971 2 413 5059  
E-mail: [ethics@mubadala.ae](mailto:ethics@mubadala.ae)  
Post: Mubadala Investment Company PJSC  
Ethics & Compliance Office  
PO Box 45005  
Abu Dhabi, UAE

## Appendix 2

### Example of Notification Message

The Mubadala Group shall inform Mubadala Group Personnel and candidates of the purposes for which their Personal Data is collected, used and disclosed. Find below a sample of a notification message that may be sent before Processing Personal Data. Mubadala Group collection, Processing, use, sharing and transferring of Personal Data is limited to the purposes for which notification has been made to Data Subjects.

Mubadala collects and uses Personal Data (including sensitive data such as medical data) to administer human resource and benefits programs, to aid in compliance with government and regulatory activities and requests, and for other business purposes that require the transfer of personal information to subsidiaries and third party business partners.

Personal Data that is collected and used by Mubadala also may need to be shared with other companies within Mubadala's group or with third party service providers (including, but not limited to, payroll administrators and benefits providers) in the United Arab Emirates and other countries. Personal data will be transferred only on an as-needed basis and only to fulfil a legitimate business purpose or legal requirement.

Mubadala will take reasonable measures to keep your Personal Data private, confidential, and accurate.