# Personal Data Protection Policy

**Content:** Overview of personal data protection requirements

**Applicable to:** All matters related to the collection, processing and storage of personal data collected in the course of OPEC Fund's operations

**Sponsor:** GCLSD

**Cleared by and date:**
RMC 07.02.2022 and
ARC 22.02.2022

**Approved by and date:**
Governing Board, 16.03.2022

**Next Review:** 2 years from approval date

**Contact:**
GC-Legal@opecfund.org

# PERSONAL DATA PROTECTION POLICY

## SECTION I: PURPOSE

This Personal Data Protection Policy ("Policy") aims to encode the commitments to and enhance the transparency of OPEC Fund's Personal Data Processing activities in line with our stakeholder's data privacy rights. This is in line with the OPEC Fund's general commitment to transparency and accountability, which are part of its core values and are relevant to the fulfilment of its development mandate.

This Policy is not an express or implied waiver of OPEC Fund's privileges and immunities under the Agreement Establishing the OPEC Fund, international conventions, or any applicable law. It does not and is not intended to provide any contractual or other rights to any party.

## SECTION II: APPLICATION

This Policy shall apply to all matters related to the Processing of Personal Data collected in the course of OPEC Fund's operations in line with the scope listed in section IV.

## SECTION III: DEFINITIONS

Capitalized words and acronyms used in this Policy shall have the meanings ascribed to them below:

- **Compliance Function** - Organizational unit responsible for facilitation of Compliance Framework and overseeing implementation of Compliance policies
- **Asset and Core Asset** – Asset is either software or hardware within an information technology environment. A Core Asset is an Asset that has been prioritized by the Information Security Function due to its underlying related information security risk (e.g. need for core operations as it relates to business continuity, reputational risk if related information breached, etc.).
- **Asset Owner** – For the purposes of Personal Data Protection, the Asset Owner is defined as the OPEC Fund employee responsible for the Asset within which Personal Data is Processed. For the broader purpose of Information Security, Asset Owner is defined as the person responsible for the day-to-day management of assets. This includes not only electronic and hard copy information but also hardware, software, services, people and facilities. For synergy purposes, the Asset Owner managing Personal Data Protection and Information Security requirements will be the same individual.
- **Data Subject**- An identified or identifiable natural person, whose Personal Data are Processed by the OPEC Fund.

- **DFIs** – Development Finance Institutions
- **Governance Documents** - OPEC Fund's policies, frameworks, strategies, directives, rules, procedures, guidelines, and related governance documents
- **MDBs** – Multilateral Development Banks
- **OPEC Fund** - The OPEC Fund for International Development
- **Personal Data**- any information relating to a natural person ('data subject'), who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, specific references (e.g. date of birth, place of birth, first name), an identification number (e.g. social security number), location data or to one or more factors specific to the identity (e.g. physical, genetic, economic, cultural).
- **Process** - any operation performed on personal data, including collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, aggregation, restriction or erasure. Any handling of data is considered Processing
- **Records of Processing (RoP)** – document management system which includes details on how Personal Data is Processed (e.g. what data is used, how it is used, for what purpose, etc.)

## SECTION IV: PRINCIPLES

Personal data within the OPEC Fund is to be managed based on the following principles:

1. **Legitimacy, Fairness, and Transparency:** Personal Data within the OPEC Fund is Processed in a legitimate, fair and transparent manner, specifically all Personal Data used:
    a. reasonably believed to be necessary for pre-contractual measures requested by a Data Subject (e.g. initiation of business with potential customers, job applicants), performance of a contractual obligation, or
    b. is reasonably necessary in order to protect the vital interests of the Data Subject or another natural person (e.g. for the purposes of preventing fraud), necessary for a broader compliance requirement, or reasonably necessary to enable the OPEC Fund to carry out its mandate,
    c. has been collected with consent from the Data Subject, the request was in a clear manner using simple language and was not unnecessarily connected to an unrelated contractual obligation

2. **Purpose Limitation.** Personal Data is Processed in a manner that is reasonably related to the objectives described and justified, and not further Processed in a manner that is incompatible with the original purpose(s) for which it was collected. Processing for archiving purposes, research, or statistical purposes shall not be considered incompatible with the original purpose.

3. **Data Minimization.** Personal Data requested and collected shall be limited and proportionate to only what is necessary.

4. **Accuracy.** Personal Data is recorded with reasonable care in order to be accurate, and where necessary, updated to ensure it fulfils the legitimate purpose(s) for which it is Processed.

5. **Storage Limitation.** Personal Data is stored for no longer than is reasonably necessary for the purposes for which it is Processed.

6. **Integrity and Confidentiality.** Personal Data is Processed in a manner that reasonably ensures its appropriate security (protection against unauthorised or unlawful processing and against accidental loss, destruction or damage) using appropriate technical/organisational measures

7. **Transfer of Personal Data.** Personal Data is only transferred to third parties for legitimate purposes and with appropriate regard for the protection of Personal Data.

8. **Data Subjects Requests.** Under the condition that the Data Subject has proven their identity, and to the extent permissible (i.e. required for compliance or legal/contractual reason), or feasible (i.e. technically possible and does not require disproportionate effort) the following Data Subject requests shall be observed:
    a. request of access - know where their Personal Data is being processed,
    b. request to rectification - request that their Personal Data be corrected/updated,
    c. request "to be forgotten"– request that their personal data be erased,
    d. request to object - to the processing of Personal Data on legitimate compelling grounds or to appeal to the Personal Data Protection Appeals Committee any decision taken by the OPEC Fund not to fulfil a Data Subject request

9. **Accountability**. To oversee compliance with this Policy the following mechanisms are enacted:
    a. implementation of Directives, trainings, controls and control testing to manage high quality adherence to data confidentiality and privacy principles
    b. establishment of a process, subject to reasonable limitations and conditions, in order to be able to fulfil Data Subjects requests, including an appeals mechanism via the Personal Data Protection Appeals Committee, if the Data Subject reasonably believes that the individual's Personal Data has been Processed in violation of this Policy

10. **Provision for Review:** This Policy will be subject to periodic review, revision to ensure that international best practices fit for purpose for the OPEC Fund are followed, that the Policy remains relevant to stakeholders and is comparable to similar policies of other MDBs/DFIs, to the extent applicable to OPEC Fund's context.

11. **Cost Implications:** Similar to peer multilateral development banks, the OPEC Fund has an over-riding mandate of providing development funds to sovereign borrowers at the lowest possible cost. Accordingly, and in light of the OPEC Fund being exempt from national and international regulation with regards to the protection of Personal Data, the principles above will be applied as long as doing so does not result in disproportionate cost to the OPEC Fund.

The OPEC Fund in applying a risk based approach to managing Personal Data Protection, applies these principles to Core Assets and corporate procurement.

## SECTION V: ROLES

Roles and responsibilities are organized along the Three Lines of Defense Model (3LOD) with segregated responsibilities with independent layered oversight. Below is a **high-level description** of roles. Responsibilities managing specific obligations can be found within the Personal Data Protection Directive document.

**First Line of Defense (FLOD):**

- All operating units are to be aware of the Personal Data Protection requirements and to inform Compliance if they are Processing Personal Data
- All operating units that are Processing Personal Data are to assign an Asset Owner, responsible for ensuring compliance with Personal Data Protection Requirements. If gaps are identified, Asset Owner are required to develop and implement a treatment plan to close the deviation
- Asset Owners are required to continuously maintain a Records of Processing (RoP) database which includes details on how Personal Data is Processed
- Asset Owners are required to respond to Data Subject requests in timely and high quality manner as instructed by Compliance Function
- Asset Owners are to inform Compliance Function immediately in any instances of Personal Data Protection breaches

**Compliance Function - Second Line of Defense (SLOD):** As an independent controlling function, provides oversight and facilitates the Personal Data Protection framework, including but not limited to:

- Defining requirements, facilitating the establishment of Governance Documents and controls aimed at Personal Data Protection and monitoring their effectiveness

- Facilitating the development and maintenance of a RoP document management system across the OPEC Fund
- Facilitating the implementation of Data Subject requests (i.e. distribution of requests to Asset Owners, collection of responses, communication to Data Subjects)
- Validating Asset Owner treatment plans in case Personal Data Protection gaps are identified
- Training of employees for the purpose of understanding Personal Data Protection requirements
- Reporting results of Personal Data Protection framework within Compliance report

**Internal Audit Function - Third Line of Defense (TLOD)** as an autonomous unit, oversees the entire Personal Data Protection framework via periodic audits.

**Stakeholders** – the following functions have roles that support the FLOD in the Personal Data Protection Framework implementation:

- Information Security Management Function – facilitation the implementation of Information Security Standards to support the integrity and minimization of Personal Data
- Operational Risk Management - facilitating the application of Operational Risk Self Assessments and the identification of Personal Data Protection gaps/risks
- Administrative Services – facilitating the application of Standard Personal Data Protection Disclaimer Terms within outsourcing contracts

Each party has a dedicated but segregated role that is contributing to an effective Personal Data Protection control environment. Further details of specific responsibilities can be found in the Personal Data Protection Directive document.

## SECTION VI: POLICY ALIGNMENT

Where applicable, OPEC Fund's Governance Documents should be updated to align with this Policy in order to facilitate its implementation. Any reference in this Policy to other Governance Documents shall include amendments to those documents.

## SECTION VII: IMPLEMENTATION AND REPORTING

The Compliance Function shall be responsible for the effective implementation of this Policy, in accordance with the provisions of this Policy and related Directive.

The Compliance Function shall report to the committees overseeing the Compliance Framework, as defined in the Compliance Policy.

## SECTION VIII: ENTRY INTO FORCE

This Policy shall become effective as of the approval date.

## SECTION IX: AMENDMENT

Amendments to this Policy shall follow the procedure set forth in Section V or Section VI of the Policies and Procedures Framework, as applicable.