AIIB Directive on Personal Data Privacy

June 22, 2022

1. OVERRIDING OBJECTIVE

1.1 This Directive establishes rules and procedures governing the Processing of Personal Data by the Asian Infrastructure Investment Bank (AIIB or the Bank) pursuant to the Policy on Personal Data Privacy (PPDP or Policy) to ensure effective and efficient implementation of this Policy.

1.2 The exercise and interpretation of this Directive shall seek to give effect to this overriding objective. In the event of conflict or inconsistency between this Directive and the PPDP, the latter shall prevail.

2. DEFINITIONS

2.1 The capitalized terms used in this Directive have the meaning set forth in the PPDP. Other capitalized terms are defined in Annex I.

2.2 Words importing the singular include the plural and vice versa, and all verbs include their conjugations.

3. OPERATIONALIZATION OF THE PRINCIPLES OF PPDP

3.1 Legitimate and Fair Processing of Personal Data

Processing of Personal Data by the Bank is considered as legitimate and fair only if, and to the extent, that at least one of the following criteria is met:

(a) Consent is obtained from the Data Subject for Processing of their Personal Data for one or more specific purposes;
(b) Processing is necessary for the Bank's performance of a contract, including a contract to which the Data Subject is a party or in order for the Bank to take steps at the request of the Data Subject prior to entering into such contract;
(c) Processing is necessary for the Bank to comply with a binding obligation or commitment, including compliance with the Bank's internal legal framework comprising policies, directives, administrative guidance and other rules and procedures, as well as any other applicable obligations to which the Bank may be subject;
(d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; or
(e) Processing is consistent with, or reasonably necessary to the fulfillment of AIIB's functions, mandate or purpose, including the performance of a task carried out by the Bank in the public interest or in the execution of the functions of the Bank as set out in AIIB's Articles of Agreement and other constituent instruments of the Bank or is necessary for establishing and asserting the status, privileges, immunities and exemptions of the Bank.

3.2 Processing of Personal Data for Specified Purposes

Personal Data shall be processed for specified and legitimate purposes, which shall be consistent with the mandate of the Bank and determined prior to the time of collection. Subject to Section 3.1 of this Directive, the Bank shall Process different types of Personal Data for various purposes. The Bank's Processing of Personal Data shall include, but not be limited to, Personal Data:

(a) of applicants for a staff position in the Bank obtained during the recruitment process, including Pre-appointment Records;
(b) relating to Board Officials and their immediate family members as defined in the Code of Conduct for Board Officials for all purposes related to their service at the Bank;
(c) of Bank Personnel and former Bank Personnel as well as their immediate family as defined in the Code of Conduct for Bank Personnel for all purposes necessary for the implementation of, and adherence to, the terms and conditions of their appointments with the Bank; and
(d) of International Advisory Panel members, individual experts, contractors, clients or third parties as well as with respect to any natural or legal person connected with such experts, contractors, clients or third parties, for the purpose of performance of the contract between the Bank and such experts, contractors, clients or third parties.

3.3 **Maintaining Accuracy of Personal Data**

Reasonable efforts shall be made to Process Personal Data with accuracy and to ensure such Personal Data is current. Personal Data that is retained by the Bank shall be reassessed periodically in order to ensure such accuracy.

3.4 **Retention Schedules for Personal Data**

The Records and Information Management Unit (RIM) of the Facilities and Administration Services Department (FAS) shall, in consultation with the Primary Office of Records that Processes Personal Data, incorporate the length of time for retention of Personal Data into existing retention schedules for the time required to achieve the purposes for which the Personal Data was collected. Personal Data shall only be retained permanently in the Bank's filing system if the criteria under the Bank's Directive on Records and Information Management and Administrative Guidance on Records and Information Management are met.

3.5 **Security and Confidentiality of Personal Data**

The Bank shall take reasonable steps to ensure:

(a) the appropriate ongoing security and confidentiality of Personal Data, including by adopting reasonable measures to prevent accidental or unauthorized destruction, loss, alteration, disclosure of, access to, or use of Personal Data and the equipment used for its Processing;
(b) the ongoing integrity, availability and resilience of its Processing systems and services;
(c) that the Personal Data that is Processed by the Bank is accurate and up to date;
(d) the ability to restore availability and access to Personal Data in a timely manner in the event of physical or technical incident or a Personal Data Breach;
(e) regular testing, assessment and evaluation of the effectiveness of technical and organizational measures for ensuring the security of the Processing; and
(f) the ongoing awareness and training for Bank Personnel on measures for maintaining security and confidentiality of Personal Data.

3.6 **Processing by Third Parties**

Where the Bank requires and assigns the Processing of Personal Data to be carried out on its behalf by third parties, such third parties shall satisfy all applicable information and IT security requirements of the Bank. The Bank shall undertake to impose appropriate obligations on such third parties so as to ensure that the Processing of Personal Data by third parties provide a standard of protection equivalent to the data protection obligations set out in the PPDP and this Directive.

4. **INFORMATION TO BE PROVIDED TO DATA SUBJECTS**

4.1 The Bank shall, at the time of receipt or as soon as reasonably practicable after collection of Personal Data from a Data Subject, provide such Data Subject with the following:

(a) a notification that the Bank will Process or has Processed the Data Subject's Personal Data, together with contact details of the Data Privacy Officer (DPO);
(b) general information about the type of Personal Data Processed by the Bank and from what sources that Personal Data has been obtained;
(c) information about the specified and legitimate purposes(s) for Processing the Data Subject's Personal Data as required under Principle 2 of the PPDP*;*
(d) general information that the Bank may transfer Personal Data to third parties, provided that such third parties agree to comply with a standard of protection of Personal Data that is reasonably equivalent to the level of protection established by the PPDP and this Directive;
(e) general information about the length of time for retention of the Personal Data by the Bank in accordance with the applicable retention schedule as set out in section 3.4 of this Directive;
(f) general information on: (i) the Data Subject's right to request access to their Personal Data, (ii) the Data Subject's right to request that the Bank corrects or deletes their Personal Data, and (iii) the process for a Data Subject to make such requests pursuant to Section E of this Directive; and
(g) an explanation that, in cases where the Processing is based on Consent of the Data Subject, the Data Subject may withdraw their Consent at any time, without affecting the validity of the Processing of their Personal Data based on their Consent before its withdrawal.

5. **INITIAL REQUEST BY DATA SUBJECT FOR ACCESS, CORRECTION OR DELETION OF PERSONAL DATA**

5.1 A Data Subject who provides sufficient evidence of being the relevant Data Subject may request to access, correct or delete their Personal Data Processed by AIIB (Initial Request) as follows:

(a) Access: Data Subjects shall have the right to obtain information from the Bank as to whether or not their Personal Data is being or has been Processed by the Bank, and, where that is the case, to access information on (i) what Personal Data concerning them is or has been Processed by the Bank, (ii) the purpose of such Processing and the types of the Data Subject's Personal Data Processed by the Bank, and (iii) the length of time for retention of the Personal Data by the Bank.
(b) Correction: Upon providing satisfactory evidence to demonstrate that their Personal Data Processed by the Bank is inaccurate, the Data Subject may request to update or correct such Personal Data.

(c) Deletion: Data Subjects may request deletion of their Personal Data: (i) if they can provide satisfactory evidence that such Processing does not comply with the PPDP, or (ii) where the only legitimate basis for Processing is Consent, the Data Subject has submitted written notification to withdraw their Consent on which the Processing was based.

5.2 To make an Initial Request under section 5.1 of this Directive, a Data Subject shall submit a completed electronic request form to the DPO through the Bank's website. The Data Subject shall indicate with reasonable specificity what Personal Data is being sought to enable the Bank to locate it. All Initial Requests shall be submitted in English.

5.3 Following the submission of an Initial Request under section 5.2 of this Directive:

(a) the DPO shall acknowledge receipt of such request not later than five (5) Working Days following its receipt;
(b) the Director General, Facilities and Administration Services (DG, FAS) shall make a decision on whether or not to grant the Initial Request and inform the Data Subject of such decision not later than thirty (30) Working Days following its receipt or, if a delay is expected, provide an explanation for such delay within the aforesaid thirty (30) Working Day period. Where the DG, FAS decides that the Initial Request cannot be acceded to under the PPDP and this Directive, the DG, FAS shall provide an explanation for their decision to the Data Subject within this period.

5.4 When considering requests by a Data Subject, the Bank shall be entitled to take into account any approved Derogations under section 4 of the PPDP.

6. GENERAL EXCEPTIONS

6.1 A request under Section E of this Directive by Data Subjects to access Personal Data shall be limited only to Personal Data within the Bank's control.

6.2 The Bank shall not be required to comply with blanket requests, or to gather, extract or recreate Personal Data that is not under the Bank's control.

6.3 The Bank shall withhold or redact information from a response where the disclosure of the same falls within one of the exceptions to disclosure set out in section 8 of the Bank's Policy on Public Information (PPI).

6.4 Personal Data contained in the Archival Records held in the Bank's Archives and Records System shall not be updated or deleted, in order to preserve the integrity of the Bank's Records and Archives.

7. APPEAL AGAINST DENIAL OF INITIAL REQUEST

7.1 A Data Subject whose Initial Request to access, correct, or delete Personal Data under Section E of this Directive is denied shall have recourse to appeal such a decision by submitting an appeal request form on AIIB's website within sixty (60) Working Days following the communication of the decision by DG, FAS regarding the Initial Request. Any appeal submitted beyond the aforesaid period shall not be considered.

7.2 The Bank shall acknowledge receipt of the appeal not later than five (5) Working Days following such receipt.

7.3 The President shall appoint an external data privacy expert (Independent Expert) for the purpose of reviewing and making a recommendation to the President regarding the Data Subject's appeal under this Section G of the Directive.

7.4 The DPO shall ensure the Independent Expert has sufficient documentation and details pertaining to the request. The Independent Expert shall review the appeal, provided that they are satisfied that the Data Subject has:

(a) demonstrated that the Initial Request was submitted in accordance with the procedures set forth in this Directive; and
(b) provided a reasonable argument that the Bank has violated the PPDP or this Directive by declining the Initial Request.

7.5 The Independent Expert shall complete their review and submit their written recommendation, including the reasoned basis for such recommendation, to the President, not later than thirty (30) Working Days after receipt of the appeal whether or not to grant the Initial Request to which the appeal relates.

7.6 The President shall issue a final decision to the Data Subject not later than fifteen (15) Working Days after receipt of the recommendation from the Independent Expert.

8. MANAGING PERSONAL DATA BREACHES

8.1 The Bank shall adopt a procedure setting out the process to be followed by the Bank in case of a breach or suspected breach of data leading to the accidental or unauthorized destruction, loss, alteration, disclosure of, or access to, Personal Data Processed by the Bank. Such Personal Data breach procedures shall address, among other things, appropriate reporting channels, review or investigations of incidents, technical responsive measures and notifications to Data Subjects.

8.2 If a Personal Data Breach occurs and, in the view of the Bank, it is likely to result in a high risk of the rights of Data Subjects being violated, the Bank shall inform the concerned Data Subjects of the Personal Data Breach without undue delay, except that the Bank shall be absolved from such obligation if any of the following conditions are met:

(a) the Bank has implemented reasonable and appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular such measures that render the Personal Data affected by the Personal Data Breach unintelligible to any person who is not authorized to access it;

(b) the Bank has taken subsequent remedial measures which minimize the risk of the rights of the affected Data Subjects being violated such that the Personal Data Breach is no longer likely to result in such risk materializing; or

(c) the Bank informing the Data Subject would involve disproportionate effort (one that would make it exorbitantly infeasible for notification) against the risk to the rights of Data Subjects.

9. ROLES AND RESPONSIBILITIES

9.1 The DG, FAS shall be responsible for issuing the required guidelines and procedures related to this Directive for the adoption of effective and consistent Personal Data Privacy oversight structure and practices within the Bank.

9.2 The DPO shall manage the daily activities related to the Personal Data Processed by the Bank. The Head of RIM, FAS shall be appointed as the DPO with the overall responsibilities to implement the PPDP and this Directive.

9.3 The DPO shall carry out responsibilities including but not limited to (a) providing daily advice and guidance on Personal Data privacy matters to relevant Bank Personnel, (b) handling and responding to requests for information from Data Subjects, (c) providing advice and support on the remediation of incidents of Personal Data Breaches, (d) implementing technical and organizational measures, such as data minimization and Pseudonymization, development and maintenance of a centralized Personal Information Bank (PIB) and a Data Protection Impact Assessment (DPIA), deploying appropriate IT systems and tools, (e) maintaining retention schedules and safe disposition procedures for Personal Data, (f) organizing internal trainings for Bank Personnel and creating awareness within the Bank to mitigate risks relating to Personal Data, and (g) establishing and maintaining mechanisms for monitoring and reporting the Bank's compliance with this Directive.

9.4 Bank Personnel shall have a responsibility to comply with and apply the PPDP and this Directive in the execution of their official duties. They shall Process Personal Data only for specified and legitimate purposes, and in doing so shall adhere to the provisions of the PPDP and this Directive.

9.5 The heads of each Business Unit shall ensure that privacy measures are integrated into their respective business and operational activities. The head of each Business Unit that Processes Personal Data shall also identify a Bank Personnel in the Business Unit who shall act as the focal point of contact for queries raised or received by the DPO for the purpose of reviewing Data Subjects' requests or appeals or from other Bank Personnel in relation to the Personal Data Processed by that Business Unit.

10. REPORTING

10.1 The Bank shall carry out a review on the implementation of this Directive after three (3) years following the coming into effect of this Directive, and if appropriate, propose revisions to any of its provisions. In addition, the President shall, on an annual basis, submit a report to the Board of Directors setting out its observations on the implementation of this Directive. Such report shall also include a summary of the activities of the appeal mechanism under Section G of this Directive as well as the cases of Personal Data Breach.

11. ACCOUNTABILITY AND RESPONSIBILITY

11.1 The President may waive any provision of this Directive that does not derive from the PPDP.

ANNEX 1: DEFINITIONS

Archival or Historical Records
As defined in the Administrative Guidance on Records and Information Management, Archival or Historical Records refer to original materials of the Bank in any format that capture and show the history of the institution which shall be kept permanently and made available to the public.

Active Records
As defined in the Directive on Records and Information Management, Active Records refer to those Records that are created or received during the Bank's activities or work and are currently in frequent use.

Bank Personnel
As defined in the Code of Conduct for Bank Personnel, Bank Personnel means the President, Vice-Presidents, staff with fixed-term appointments, consultants with short-term and long-term appointments, and other personnel employed under contracts with outside firms to the extent provided for in such contracts.

Board Officials
As defined in the Code of Conduct for Board Officials, Board Officials mean all Directors and Alternate Directors of the Bank as provided in the Articles of Agreement, and all Temporary Alternate Directors of the Bank as provided in Section 10 (b) of the By-Laws. Board Officials shall also include Constituency Representatives and Alternate Constituency Representatives as provided in Section 12 of the Rules of Procedure of the Board of Directors.

Business Application
As defined in the Directive on Records and Information Management, Business Application refers to the specialized systems used by the Bank that process information capturing, storing, retrieving, communicating, transforming to support one or several business objectives.

Business Unit
As defined in the Directive on Business Continuity, Business Unit means a Vice-Presidency, Office, Department or equivalent unit of the Bank, or discrete subcomponent thereof.

Data Privacy Officer (DPO)
The Head of RIM, FAS is the Data Privacy Officer (DPO) with the overall responsibilities to implement the PPDP and this Directive and shall carry out duties set out in section 9.2 of this Directive.

Data Protection Impact Assessment (DPIA)
Means the assessment of the impact of the envisaged processing activities on the protection of Personal Data and on the rights of the Data Subject, aimed at identifying mitigation measures to avoid or minimize impacts if any.

Initial Request
For purposes of this Directive, an Initial Request is a request from a Data Subject to obtain access to, correction of, or deletion of their personal data in accordance with Section E of this Directive.

Personal Data Breach
Means a breach of security of Personal Data leading to the accidental or unauthorized destruction, loss, alteration, disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Pseudonymization
Means any operation or set of operations performed on Personal Data, whether by automated means or manually, such collection, recording, structure, consulting, retrieving, using, transferring, disclosing, sharing or otherwise making available, or deleting.

Pre-appointment Records
Means documents obtained by the Bank for use in making recruitment decisions, including letters of references, interview notes and candidate assessments.

Primary Office of Records
As defined in the Administrative Guidance on Records and Information Management, Primary Office of Records refers to the Business Unit that is principally accountable for the creation and/or maintenance of a particular class of Records of a function, activity or transaction of the Bank.

Records
As defined in the Directive on Records and Information Management, Records mean information in any format or medium, that is created or received by the Bank in conducting its business and/or delivering functions, that document evidence of any action or transaction.

Working Day
For purposes of this Directive, a Working Day is a day when the Bank's headquarters are open for business; it does not include weekends or the Bank's official holidays.