

**DIRECTIVE**

**Personal Data Protection**

29 April 2021

## Personal Data Protection

### Section I: Purpose

This Directive sets out the rights and obligations of Data Subjects and the Bank in relation to the Processing of Personal Data and the measures which the Bank will take to monitor the implementation and application of, as well as compliance with, the provisions of this Directive.

### Section II: Definitions and Terms

Unless otherwise defined below, capitalised terms used in this Directive shall have the meaning as defined in the Personal Data Protection Policy.

<b>Agreement Establishing the Bank</b>	means the Agreement Establishing the European Bank for Reconstruction and Development which was signed in Paris on 29 May 1990 and entered into force on 28 March 1991.
<b>Board Officials</b>	has the meaning given to it in the Code of Conduct for Officials of the Board of Directors, as amended from time to time.
<b>Code of Conduct for EBRD Personnel</b>	means the Code of Conduct for EBRD Personnel adopted by the Board of Governors, as amended from time to time.
<b>Code of Conduct for Board Officials</b>	means the Code of Conduct for Officials of the Board of Directors adopted by the Board of Governors, as amended from time to time.
<b>CDRP</b>	means the Directive on the Conduct and Disciplinary Rules and Procedures, as amended from time to time.
<b>Dependant</b>	has the meaning defined in the Directive on General Provisions and Glossary of Term for the Staff Handbook, as amended from time to time.
<b>Dispute Resolution Procedures</b>	means the Directive on the Administrative Review Process, the Directive on the Appeals Process and the Procedure on the Appeals Process, each as amended from time to time, as applicable.
<b>Enforcement Policy and Procedures</b>	means the Enforcement Policy and Procedures, as amended from time to time.
<b>Independent Project Accountability Mechanism</b>	means the independent project accountability mechanism established under the Project Accountability Policy, as amended from time to time.
<b>Pre-appointment Records</b>	means documents obtained by the Bank for use in making recruitment decisions, including letters of references, interview notes and candidate assessments.
<b>Personal Data Breach</b>	means a breach of security leading to the accidental or unauthorised destruction, loss, alteration, disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
<b>Personal Data Management Officer</b>	means the Staff Member assigned to carry out duties set out in paragraph 15 of Section IV of this Directive.

<b>Personal Data Protection Directive</b>	means this Personal Data Protection Directive, as amended from time to time.
<b>Personal Data Protection Policy</b>	means the Personal Data Protection Policy, as amended from time to time.
<b>President</b>	means the President of the Bank.
<b>Recipient</b>	means a natural or legal person, including, without limitation, a public authority, agency or another body, other than a Data Subject, to which Personal Data are disclosed.
<b>RWP</b>	means the Procedure on a Harassment-free and Respectful Workplace, as amended from time to time.
<b>Staff Handbook</b>	means the compendium of policies, rules, directives and procedures governing the organisation, appointment and dismissal of Staff Members of the Bank.
<b>Staff Member</b>	has the meaning defined in the Directive on General Provisions and Glossary of Terms for the Staff Handbook, as amended from time to time.
<b>Terms and Conditions of Employment</b>	means the terms and conditions regulating the employment relationship between the Bank and a Staff Member or former Staff Member.
<b>Vice-President</b>	means a person appointed by the Board of Directors to serve as a Vice-President of the Bank, in accordance with the Agreement Establishing the Bank and the By-Laws of the Bank.

### Section III: Legal Basis

Personal Data Protection Policy.

### Section IV: Scope

#### 1. Applicability

This Directive applies to all Personal Data Processed by the Bank.

#### 2. Lawfulness of Processing Personal Data

Personal Data shall be Processed by the Bank only if and to the extent that at least one of the following applies:

- (a) the Data Subject has given consent to the Processing of their Personal Data for one or more specific purposes;
- (b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

- (c) Processing is necessary for compliance with the Bank's policies, rules, directives 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;
- (e) Processing is necessary for the performance of a task carried out by the Bank in the public interest or in the execution of the functions of the Bank set out in the Agreement Establishing the Bank;
- (f) Processing is necessary for establishing and asserting the status, privileges, immunities and exemptions of the Bank.

### **3. Purposes of Processing of Personal Data**

Subject to paragraph 2 of this Section IV, the Bank shall Process different types of Personal Data for various purposes. These include, but shall not be limited to, Personal Data:

- (a) of applicants for a job in the Bank obtained during the recruitment process, including Pre-appointment Records;
- (b) of Board Officials and/or their dependants for all purposes related to the Board Official's service at the Bank, as well as benefits, allowances and insurance provided by the Bank;
- (c) of the President, the Vice-President, the Chief Evaluator, the Head of the Independent Project Accountability Mechanism and/or their dependants for all purposes related to their service at the Bank, as well as benefits, allowances and insurance provided by the Bank;
- (d) of Staff Members, former Staff Members and/or their Dependants for all purposes necessary for implementation and adherence to the Terms and Conditions of Employment of the Staff Member or former Staff Member upon signature of a letter of appointment by the Staff Member and entering into employment with the Bank and following termination of such employment; and
- (e) of an individual expert, contractor, consultant, client, intern or third party or, where they are a legal entity, of any natural person connected with such expert, consultant, contractor, client, or third party, for the purpose of performance of the contract between the Bank and such expert, contractor, consultant, client, intern or third party .

### **4. 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 unauthorised destruction, loss, alteration, disclosure of, or access to, or use of Personal Data and the equipment used for its Processing;

- (b) the ongoing integrity, availability and resilience of 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 organisational measures for ensuring the security of the Processing;
- (f) the ongoing awareness and training for Staff Members on Personal Data management.

## **5. Retention Schedules for Personal Data**

The department of the Bank responsible for information management shall, in consultation with each department that Processes Personal Data, incorporate the length of time for retention of Personal Data into existing retention schedules.

## **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 (legal entities or individuals), such third parties will have to satisfy information and IT security requirements of the Bank. The Bank shall ensure that it contractually imposes obligations on such third parties so that the Processing of Personal Data by third parties can (i) meet the requirements of the Personal Data Protection Policy and this Directive and (ii) ensure, as a minimum, a standard of protection of the Personal Data equivalent to the level of protection established by the Personal Data Protection Policy and this Directive.

## **7. Provision of Personal Data**

Data Subjects shall (i) provide adequate and accurate Personal Data, and (ii) promptly notify the Bank of any changes to such Personal Data, when the changes occur.

## **8. Information to be provided to Data Subjects at the time of collection or following the receipt of their Personal Data**

Subject to paragraph 10 of this Section IV, the Bank shall, at the time of receipt of the Personal Data from the Data Subjects or, where Personal Data is received from third parties, within reasonable time after the receipt of Personal Data from such third parties, provide Data Subjects with all of the following information:

- (a) notification that the Bank Processes Personal Data, the Bank's contact details as well as the contact details of the Personal Data Management Officer;
- (b) the types of Personal Data Processed by the Bank;
- (c) the purposes of the Processing for which Personal Data is obtained by the Bank, as set

out in paragraph 3 of this Section IV, as well as the express basis for Processing, as set out in paragraph 2 of this Section IV;

- (d) categories of Recipients of Personal Data Processed by the Bank;
- (e) the possibility that the Bank may transfer Personal Data to third parties provided that such third parties comply with a standard of protection of Personal Data equivalent to at least the level of protection established by the Personal Data Protection Policy and this Directive;
- (f) general information about the periods for which various categories of the Personal Data will be stored by the Bank in accordance with the relevant retention schedule (as described in paragraph 5 of this Section IV);
- (g) information about Data Subject's rights to (i) request to access their Personal Data, (ii) request that the Bank rectifies their Personal Data, and (iii) lodge a complaint in relation to the Processing of their Personal Data by the Bank before the Bank's panel established for the purpose of reviewing such complaints;
- (h) explanation that where the Processing is based on consent from the Data Subject, the existence of the right to withdraw consent at any time, without affecting the express basis of Processing based on consent before its withdrawal;
- (i) whether the provision of Personal Data is a requirement under the Bank's policies, rules, directives and procedures, or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
- (j) to the extent applicable, information about the existence of any automated decision-making and information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subjects; and
- (k) if the Personal Data is not collected from the Data Subject and is received from third parties, the sources from which the Personal Data can be originated, subject to any confidentiality undertakings entered into by the Bank.

## **9. Access to and requests for rectification of their Personal Data by Data Subjects**

Subject to paragraph 10 of this Section IV, a Data Subject shall have the right, upon request, to obtain confirmation from the Bank as to whether or not their Personal Data is being processed, and, where that is the case, to access their Personal Data Processed by the Bank and the following information:

- (a) the purposes of the Processing of their Personal Data, as set out in paragraph 3 of this Section IV;
- (b) the type of Personal Data concerned;

- (c) the Recipients or categories of Recipients of their Personal Data;
- (d) where possible, the period for which the Personal Data (for each category) will be stored in accordance with the relevant retention schedule (as described in paragraph 5 of this Section IV);
- (e) information about their rights to (i) request to access their Personal Data, (ii) request that the Bank rectifies their Personal Data, and (iii) lodge a complaint in relation to the Processing of their Personal Data by the Bank before the Bank's panel established for the purpose of reviewing such complaints;
- (f) if the Personal Data has not been collected from the Data Subject and is received from third parties, the source from which the Personal Data originated, subject to any confidentiality undertakings entered into by the Bank;
- (g) the existence of any automated decision-making and, if such decision-making is involved in the Processing of the Personal Data of the Data Subject, information about the logic involved, as well as the significance and the envisaged consequences of such Processing for that Data Subject; and
- (h) where applicable, the fact that the Bank intends to transfer or has transferred Personal Data to third parties subject to such third parties complying with a standard of protection of Personal Data equivalent to at least the level of protection established by the Personal Data Protection Policy and this Directive.

If the relevant information has already been provided to the Data Subject pursuant to paragraph 8 of this Section IV and the information remains unchanged, the Bank may refer the Data Subject to the previously provided information.

In the event that the Data Subject identifies inaccuracies or incompleteness in the Personal Data, they shall have the right (i) to request that the Bank rectifies such inaccuracies; or (ii) to supplement the Personal Data, as appropriate, for completeness.

#### **10. Restrictions on the right to information and the right to access**

The Bank shall have no obligation to provide Data Subjects with confirmation or information about the Processing of their Personal Data, as set out in paragraphs 8 and **Error! Reference source not found.** above, if:

- (a) the Processing is for the purposes of the prevention and detection of crime;
- (b) the Processing is for the purposes of inquiries and investigations into misconduct pursuant to the Bank's CDRP, the Code of Conduct for EBRD Personnel or the Code of Conduct for Board Officials or for the purposes of assessments of improper behaviour pursuant to the RWP, or inquiries and investigations under the Enforcement Policy and Procedures;

- (c) the Processing is for the purposes of the internal Dispute Resolution Procedures, the processing and review of complaints filed with the Independent Project Accountability Mechanism, or the commencement and processing of enforcement proceedings pursuant to the Enforcement Policy and Procedures;
- (d) the Processing is for the purpose of integrity checks of the Bank's potential or existing clients, contractors, partners or other parties;
- (e) disclosure of the Personal Data is required in accordance with the Bank's policies, rules, directives and procedures to the extent that complying with the obligation would prevent the Bank from disclosing the Personal Data;
- (f) disclosure of the Personal Data is necessary for the purposes of, or in connection with (i) legal proceedings, including prospective or threatened legal proceedings; (ii) obtaining legal advice; or (iii) establishing, exercising or defending legal rights, in each case to the extent that complying with the obligation would prevent the Bank from disclosing the Personal Data;
- (g) the Processing is for the purposes of management forecasting or management planning in relation to the Bank's operations or activities, to the extent that complying with the obligation above would be likely to prejudice the conduct of the Bank's operations or activities; and
- (h) the Personal Data relates to the receipt or provision of confidential references including confidential reference checks carried out as part of the recruitment process.

## **11. Notification of Personal Data Breach**

If a Personal Data Breach occurs and, in the view of the Bank, it is likely to result in a high risk to the rights of Data Subjects, 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 one of the following conditions is met:

- (a) the Bank has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular those measures that render the Personal Data affected by the Personal Data Breach unintelligible to any person who is not authorised to access it;
- (b) the Bank has taken subsequent measures which minimise the risk to the rights of affected Data Subjects such that the Personal Data Breach is no longer likely to result in a high risk to the rights of Data Subjects; or
- (c) informing the Data Subject would involve disproportionate effort against the risk to the rights of Data Subjects.

## **12. Staff Members involved in the Processing of Personal Data and Personal Data related queries**



- (a) Staff Members shall Process Personal Data only for any one or more of the purposes outlined in paragraph 2, Section IV of this Directive, and in doing so shall adhere to the provisions of the Personal Data Protection Policy and the Implementing Acts.
- (b) Managing Directors shall identify a Staff Member in each department that Processes Personal Data who will act as the point of contact for queries raised by the Personal Data Management Officer, by the Bank's panel established for the purpose of reviewing Data Subjects' complaints and by other Staff Members in relation to the Personal Data Processed by that department.

### **13. Accountability**

- (a) The Managing Director, Risk Management shall adopt a procedure setting out the process to be followed by Data Subjects for submission to the Bank of requests for access, rectification or supplementation of Personal Data in accordance with the Personal Data Protection Policy and this Directive.
- (b) The Managing Director, Risk Management shall adopt a procedure setting out the process to be followed by Data Subjects for submission of complaints to the Bank for failure by the Bank to Process Personal Data in accordance with the Personal Data Protection Policy and the Implementing Acts.
- (c) The Managing Director, Risk Management shall adopt a procedure setting out the process to be followed by the Bank in case of a breach or suspected breach of security leading to the accidental or unauthorised destruction, loss, alteration, disclosure of, or access to, Personal Data Processed by the Bank.

### **14. Monitoring and Compliance**

The Bank shall establish appropriate systems and mechanisms for monitoring the implementation, application and compliance with this Directive and any Procedures adopted for the purpose of implementing this Directive.

### **15. Personal Data Management Officer**

The Managing Director, Risk Management shall assign one Staff Member to act as a Personal Data Management Officer for the Bank and to carry out the following duties:

- (a) organising and implementing internal training for Staff Members on Personal Data Management;
- (b) providing advice to the Bank and Data Subjects on the implementation, application and compliance with this Directive;
- (c) providing advice and support on the remediation of incidents involving a Personal Data Breach; and
- (d) handling, and responding to, any requests for information from Data Subjects.

**Section V: Waivers, Exceptions and Disclosure**

**Waivers**

The President may grant a deviation from a requirement of this Directive.

**Exceptions**

Not applicable.

**Disclosure**

This Directive will be publicly disclosed.

**Section VI: Transitional Provisions**

Not applicable.

**Section VII: Effective Date**

This Directive is effective on the date of its adoption.

**Section VIII: Accountable and Responsible**

The Vice-President, Risk & Compliance is accountable for this Directive.

The Managing Director, Risk Management is responsible for the implementation of this Directive.

**Section IX: Review and Reporting**

**Review**

This Directive will be reviewed annually.

**Reporting**

Not applicable.

**Section X: Related Documents**

Personal Data Protection Policy