Policy on the Protection of Personal Data

Table of Contents

1. PURPOSE & SCOPE

This document is a Policy defining the protection of Personal Data throughout the Bank's activities.

The importance of the protection of natural persons with regard to the Processing of their Personal Data as an expression of the fundamental right to privacy[1] is currently increasing. Technology, which has transformed both the economy and social life, facilitates the free flow and transfers of Personal Data, as such flows and transfers are necessary for the expansion of international trade and international cooperation. The increase in such flows and transfers has raised new challenges and concerns with regard to the protection of Personal Data.

Thus, current international best standards and practices in the area of Personal Data protection are recognized worldwide, impacting also international organizations[2], such as the Bank. The latter, being responsive to the new privacy environment, has interest in implementing Personal Data protection measures which meet the principles enshrined in current relevant international best standards and practices in the area.

In this framework, the objective of the present Policy is the adoption of appropriate measures and safeguards for the Processing of Personal Data by the Bank, so that an adequate level of Personal Data protection is ensured and compliance with current international best standards and practices is achieved. By adopting the present Policy, the Bank aspires to provide assurance that natural persons, acting either in their private capacity or as reprentatives of legal entities, can continue to engage with the Bank with due regard to the protection of their Personal Data.

The Personal Data collected by the Bank shall be kept secure via the use of administrative, organizational, technical and physical safeguards to protect it from loss, theft, misuse, unauthorized access, unauthorized disclosure, alteration or destruction. The Bank shall implement appropriate related procedures, in order to ensure the effectiveness of the implementation of the present Policy in the Bank's every-day activities.

Thlis Policy is applicable to:

a) Directors, Alternate Directors, Temporary Alternate Directors, in their capacity as members of the Board of Directors ("Board Officials");

b) The President, the Vice Presidents and the Secretary General ("Bank Officials");

c) Officers and staff of the Bank ("Staff Members");

d) Interns, experts and consultants or any other individual engaged at any given period by the Bank, to the extent set out in their terms of reference or contracts, as the case may be.

The Bank expects all of the aforementioned persons to read, understand and comply with the present Policy.

[1] Regarding the human right to privacy, see indicatively: United Nations, Universal Declaration of Human Rights, 1948, Article 12; United Nations, International Covenant on Civil and Political Rights, 1966, Article 17; United Nations, Convention on the Rights of the Child, 1989, Article 16; regarding the protection of personal data as an expression of the right to privacy, see indicatively: Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 (last updated 2013).

[2] See indicatively the response of the World Bank Group to the General Data Protection Regulation of the European Union:

http://documents.worldbank.org/curated/en/466121527794054484/text/Privacy-Board-Paper-050318-vF-05042018.txt

2. TERMS & ABBREVIATIONS

2.1 Terms

The following terms are used in this policy as respectively defined below:

"Data Subject": an identified or identifiable natural person

"Establishing Agreement": Agreement Establishing the Black Sea Trade and Development Bank (an international treaty signed in 1994 and registered with the UN pursuant to Article 102 of the United Nations Charter)

"Money Laundering": has the meaning ascribed to it under BSTDB's Anti-Fraud, Corruption, Money Laundering and Terrorism Financing, and Domiciliation of BSTDB Counterparties Policy

"Personal Data": any information relating to a Data Subject; an identifiable natural person is one who can be identified, by reasonable means, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, metadata or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

"Processing": any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

"Prohibited Practices": has the meaning ascribed to it under BSTDB's Anti-Fraud, Corruption, Money Laundering and Terrorism Financing, and Domiciliation of BSTDB Counterparties Policy

"Terrorism Financing": has the meaning ascribed to it under BSTDB's Anti-Fraud, Corruption, Money Laundering and Terrorism Financing, and Domiciliation of BSTDB Counterparties Policy

2.2 Abbreviations

The following abbreviations are used in this Policy:

Abbreviation	Full Wording of Abbreviation
DCR	Compliance and Operational Risk Management Office of the Bank
DIA	Internal Audit Department
DPO	Data Protection Officer

3. RESPONSIBILITIES

The following Business Units and Positions are responsible for the corresponding tasks:

- **DCR** shall ensure that:

- all the rules of the Bank are reviewed, so as to ensure their compliance with the present Policy, as well as the incorporation of relevant controls, as appropriate;
- all the persons of the Bank to which the present Policy is applicable are regularly trained on how to best protect Personal Data;
- the application and effectiveness of the present Policy is reviewed periodically, taking into account international best standards and practices in the area of Personal Data protection, as well as experience acquired through its implementation, in order to update it, as required.

- The Bank's **Data Protection Officer (DPO)** shall:

- inform and instruct the Bank, all persons of the Bank to which the present Policy is applicable or any third person Processing Personal Data controlled by the Bank regarding the requirements of best international practices on the protection of Personal Data;
- contribute to the drafting of the relevant Bank's rules;
- monitor compliance with best international practices on the protection of Personal Data and the rules of the Bank on the protection of Personal Data;
- provide advice on the Personal Data protection impact assessment and monitor its performance;
- act as the contact point for any internal of external person expressing concern over the protection of (his/her) Personal Data by the Bank.

- The Bank's **Head of Internal Audit Department (DIA)**, which is an independent function within the Bank and is responsible for the management and coordination of the Bank's independent accountability mechanism according to which complaints and grievances are handled, shall receive all the complaints and grievances submitted to the Bank by any party that is directly and/or significantly affected by the Bank's or its business counterparts' Personal Data protection practices.

- **All persons of the Bank to which the present Policy is applicable** shall fully comply with the principles and practices enshrined in the present Policy in their everyday operations for ensuring the protection by the Bank of Data Subjects' Personal Data.

4. POLICY

4.1 Personal Data Protection Principles and Practices for Ensuring Compliance with the Principles

The Bank recognizes the importance of the protection of Data Subjects with regard to the Processing of their personal data as a fundamental right. In this respect, the Bank complies with the following **principles governing the Processing of Personal Data**, to ensure consistent practices, aligned with current international best standards and practices for the relevant rights of the Data Subjects.

In this context, the Bank ensures that Personal Data:

- is processed fairly and in a transparent manner in relation to the Data Subject, in accordance with this Policy and the Bank's mandate, on any of the following **legal bases**:

  i) the consent of the Data Subject;

  ii) the vital or best interest of the Data Subject or of another natural person, consistent with the Bank's mandate;

  iii) the performance of a contract;

  iv) the compliance with a binding obligation of the Bank;

  v) the consistency with the Bank's mission, purpose and mandate as an international organization;

  vi) any other legal basis specifically identified by the Bank;

- is collected for one or more specified, explicit and legitimate purposes and is processed only for the purpose(s) for which it has been collected and not further processed in a manner that is incompatible with the specified purpose(s); further processing for archiving, research or statistical purposes shall not be considered incompatible with the initial purpose(s);

- is adequate, relevant and limited to the minimum data required in relation to the specified purpose(s), in accordance with the principle of proportionality;

- is accurate, and, where necessary, kept up to date, to ensure fulfilment of the legitimate purpose(s);

- is not retained for longer than is necessary for the purpose(s) for which the Personal Data was collected;

- is processed with due regard to confidentiality and is retained secure -using appropriate technical and organizational safeguards- from unauthorized or unlawful Processing, including unauthorized or accidental access, unauthorized modification, damage, loss or reasonably avoidable breaches;

- is transferred to third parties for legitimate purpose(s), provided that appropriate level of Personal Data protection has been reasonably ascertained in advance.

The Bank **ensures compliance with all the above principles by adhering to the following practices**:

- applying a Personal Data and information security management system, which covers the Bank's activities, monitors and controls the implementation of this Policy, while it also assesses the effectiveness regarding current international best standards and practices for the protection of Personal Data;
- updating its systems in accordance with privacy-by-design, where data protection and safeguards should be embedded from the beginning;
- applying procedures for satisfying the complete and effective protection of Data Subjects' relevant rights;
- explicitly informing Data Subjects regarding the Processing of their Personal Data, in accordance with sections 4.2 – 4.5 herein;
- incorporating Personal Data Processing requirements to all operational functions which are relevant to Processing;
- recognizing all internal and external interested parties and the specific requirements towards the protection of their Personal Data;

- designing, adopting and monitoring a system of indicators and targets for secure and lawful data management, in accordance with this Policy;
- specifying roles and responsibilities associated with Personal Data management;
- designating a DPO;
- giving explicit directions, in accordance with section 4.7 of the present Policy, to all the persons of the Bank within the scope of the present Policy and third parties which execute Processing of Personal Data on behalf of the Bank, for data use and data transmission;
- providing adequate resources for reasonably ensuring effective application of the present Policy;
- investing in on-going staff training and awareness on Personal Data protection issues, as well as in periodic improvement of know-how of the Staff Members;
- Periodically updating this Policy in accordance with relevant international developments.

4.2 Purposes of Collection of Personal Data, Catergories of Personal Data collected, Means of Collection and Recipients

The main purposes for which the Bank processes Personal Data are listed below:

- **Management of the Bank's lending/investing and borrowing processes:** e.g. for the evaluation of projects (such as, for example, KYC due diligence), asset recovery in case of impaired operations, preparation of legal documents, provision of legal advice and litigation etc.
- **Management of the Bank's human resources:** e.g. for employee recruitment, intern selection, administration of social security and pension schemes, training, learning and development of the employees, handling of grievances etc.
- **Administrative functions of the Bank:** e.g. for events management, collection and registration of documentation, handling of documents mainly for signature purposes, registration of consultants for Bank's operations etc.
- **Management of audit, investigations and complaints:** e.g. for the performance of internal/external audits, internal investigations regarding violations of the Bank's Code of Conduct, external investigations regarding Prohibited Practices, Money Laundering and Terrorism Financing, handling of complaints etc.

In this context and in compliance with the principles enshrined above, the Bank may collect from the relevant Data Subjects (**such as e.g. borrowers, beneficial owners, representatives, candidates, Staff Members, interns, dependents, contractors, service providers, event attendees etc.**), **directly from them or from an authorized intermediary or from publicly available sources**, relevant and necessary Personal Data including but not limited to:

- **personal information** (e.g. full name, date of birth, marital status, citizenship, address, telephone numbers etc.);
- **unique identification data** (e.g. tax/VAT number, ID/passport number etc.);
- **financial data** (e.g. source of wealth, IBAN, tax/VAT number, salary, loans etc.);
- **educational and professional data** (such as e.g. CV etc.);
- **health data;**
- **data on race/origin;**

- **religious beliefs;**
- **political beliefs and relationships;**
- **data regarding administrative and criminal investigations, administrative and criminal penalties, and other related data**.

Given the above and depending on the case, **recipients** of the above Personal Data of the aforementioned Data Subjects are primarily the following:

- the Bank's **Staff Members, Bank Officials and Board Officials**;
- the Bank's **experts and consultants** or any other individual engaged at any given period by the Bank;
- **third party providers** (e.g. insurance companies, transportation companies etc.);
- **public authorities** (e.g. ministries etc.).

4.3 Third Parties Processing Personal Data on behalf of the Bank

Whenever the Bank transfers Personal Data controlled by it to third parties for legitimate purpose(s), it shall reasonably ascertain, in advance, by all appropriate means, that an adequate degree of protection is applied by the third party. Such means may include inter alia the imposition of contractual clauses, the reservation by the Bank of the right to verify the adequacy of protection etc.

In case of absence of adequate safeguards on behalf of a third party, when the transfer of Personal Data controlled by the Bank cannot be avoided, it shall be transferred for the specific purpose(s), only on the basis of the prior consent of the Data Subject, following the provision of comprehensive information to the Data Subject on the possible risks related to such a transfer.

4.4 Retention Periods

Personal Data shall be retained only for as long as it is required, according to the Bank's legitimate interests and in accordance with its Policy on the Management of Official Records and Archives, the performance of the contract or any other specific purpose for which the Personal Data was collected and processed.

If not otherwise dictated by the Bank's legitimate interests and rules, Personal Data shall be retained for seven (7) years following e.g. the amicable termination/expiry of the (contractual) relationship, the closure of an audit/investigation, the event upon which the Personal Data was initially collected etc.

4.5 Rights of Data Subjects

The Processing of Personal Data by the Bank is carried out with transparency vis-à-vis the Data Subjects, as appropriate. Transparency includes inter alia the provision of information to the Data Subjects about the Processing of their Personal Data, as well as provision of information to the Data Subjects regarding the full spectrum of their related rights under this Policy and the mode of exercising them.

Namely, Data Subjects possess and can exercise the following rights regarding the Processing and retention of their Personal Data by the Bank:

- request information as to whether or not their Personal Data is being processed by the Bank;
- request information as to the purpose of the Processing by the Bank, the categories of their Personal Data processed and the recipients of their Personal Data;
- request verification of their Personal Data;
- request the correction of their Personal Data, when the Personal Data held by the Bank is inaccurate or insufficient;
- request the deletion of their Personal Data, in case there is no legal obligation for the Bank to keep it or if no longer necessary for the specific purpose(s) for which it was collected;
- withdraw their consent, in cases where consent is the legal basis for the lawful Processing of Personal Data by the Bank;
- object to the Processing of their Personal Data, when the Bank has no legal basis for such Processing;
- request restriction of the Processing of their Personal Data, when the Bank has no legal basis for such processing;
- request the Bank to provide them with their Personal Data in a structured, commonly used and machine-readable format, so as to transfer their Personal Data to a third party;

The Bank may restrict, where applicable, the exercise of any of the aforementioned rights, where such restriction may constitute a necessary measure to ensure safeguards, such as e.g. the prevention, investigation and detection of Prohibited Practices, Money Laundering and Terrorism Financing, the protection of the Data Subject, the protection of the rights and freedoms of others etc.

Data Subjects may exercise their aforementioned rights, by addressing the Bank's Data Protection Officer (DPO): https://www.bstdb.org/privacy, who shall acknowledge the receipt of the request and, following the review of the request, respond, without undue delay.

4.6 Complaints and Grievances

Any party that is directly and/or significantly affected by the Bank's or its business counterparts' Personal Data protection practices may submit complaints and grievances to the Bank. The latter provides the necessary means for these complaints and grievances to be communicated, processed and dealt upon in a timely, transparent and responsible manner. All the complaints and grievances are submitted to the Bank's Head of DIA, which is an independent function within the Bank and is responsible for the management and coordination of the Bank's independent accountability mechanism according to which such complaints and grievances are handled.

The complaints and grievances are submitted to the Bank in accordance with the Procedure for the Receipt, Retention and Treatment of Complaints available on the Bank's website: https://www.bstdb.org/transparency/complaints

4.7 Role of DCR and of DPO

DCR, being tasked with the protection of Personal Data by the Bank, shall ensure that:

- all the rules of the Bank are reviewed and updated, if needed, so as to ensure their compliance with the present Policy, as well as the incorporation of relevant controls, as appropriate;

- a Procedure on the Protection of Personal Data is issued in due time, upon its approval by the Management Committee;
- all the persons of the Bank to which the present Policy is applicable are regularly trained on how to best protect Personal Data;
- the application and effectiveness of the present Policy is reviewed periodically, taking into account international best standards and practices in the area of Personal Data protection, as well as experience acquired through its implementation, in order to update it, as required.

In particular, the Bank's DPO, comprising DCR Staff Member, shall:

- inform and instruct the Bank, all persons of the Bank within the scope of the present Policy or any third person Processing Personal Data controlled by the Bank regarding the requirements of best international practices on the protection of Personal Data;
- contribute to the drafting of the relevant Bank's rules;
- monitor compliance with:
  (a) best international practices on the protection of Personal Data
  and
  (b) the rules of the Bank on the protection of Personal Data, including inter alia rules on the assignment of responsibilities, on awareness-raising and on the training of staff involved in Processing operations and in the personal data-related audits;
- provide advice on the Personal Data protection impact assessment and monitor its performance;
- act as the contact point for any internal of external person expressing concern over the protection of (his/her) Personal Data by the Bank and consult/cooperate with relevant parties.

4.8 Privileges and Immunities of the Bank

The implementation of the present Policy is without prejudice to the privileges and immunities of the Bank, accorded in the Establishing Agreement.