



HAITONG

REGULATION No. COM17.R24

**Personal Data Privacy
of Haitong Bank S.A**

Approved by the Board of Directors
on 19/12/2022

TABLE OF CONTENTS

| | | |
|-----|-----------------------------------|----|
| 1. | OBJECTIVE..... | 3 |
| 2. | RECIPIENTS | 3 |
| 3. | RESPONSIBILITY | 3 |
| 4. | DISCLOSURE..... | 4 |
| 5. | PRINCIPLES | 4 |
| 6. | DEFINITIONS | 4 |
| 7. | PERSONAL DATA..... | 5 |
| 8. | CATEGORIES OF PERSONAL DATA | 6 |
| 9. | PROCESSING OF PERSONAL DATA..... | 7 |
| 10. | DATA SUBJECTS' LEGAL RIGHTS | 12 |
| 11. | ARCHIVE | 14 |
| 12. | MONITORING | 14 |
| 13. | CONTROL OF VERSIONS | 15 |

1. OBJECTIVE

Haitong Bank, S.A. (the “**Bank**”) endeavours to remain abreast of developments and comply with the measures laid down in Regulation (EU) 2016/679 (the General Data Protection Regulation or the “**GDPR**”) and in any other applicable laws, by adopting an appropriate and organised set of technical measures. This Regulation sets out the terms in which the Bank processes the Personal Data of Data Subjects, as well as the rights they can exercise, pursuant to the GDPR provisions and other applicable legislation in matters of privacy and data protection.

2. RECIPIENTS

- a. The content of this Regulation represents a minimum standard that shall apply to the Bank and its subsidiaries and branches (“**Haitong Bank Group**”).
- b. In case of conflict between any provision of this Regulation and the local laws and regulations applicable to any Bank's subsidiary or branch, the relevant local laws and regulations shall prevail.
- c. The Bank's affiliate in Brazil (Haitong Banco de Investimento do Brasil S/A) has its own privacy regulation, which is consistent with the rules of this Regulation and respects the specificities of local law.

3. RESPONSIBILITY

- a. This Regulation is prepared by the Compliance Department, alongside the Data Protection Officer (“**DPO**”).
- b. This Regulation is approved by the Board of Directors.
- c. The Compliance Department is responsible for monitoring compliance with the Regulation.
- d. This Regulation must be reviewed at least once a year or whenever any amendments thereto become necessary.
- e. For any queries in relation to the processing of Personal Data, Data Subjects should contact the DPO directly, as indicated on the Bank's website (www.haitongib.com), using:
 - the Data Protection Officer's email address: dpo@haitongib.com,
 - the mail address of the Data Protection Officer: R. Alexandre Herculano 38, 1269-180 Lisbon, Portugal.

4. DISCLOSURE

- a. This Regulation is available on the Bank's intranet and website.
- b. After any amendments are approved to this Regulation, the Compliance Department informs by e-mail all Bank's staff within 30 (thirty) days from the approval date and requests the upload of the most updated versions of the Regulation on the Bank's intranet and website.

5. PRINCIPLES

- a. This Regulation aims at clarifying the rights of the Data Subjects in relation to their Personal Data processed by the Bank.
- b. This Regulation aims at informing the Data Subjects in relation to the Personal Data processed by the Bank, namely the purposes for the collection of Personal Data, in what circumstances we share Personal Data with third parties, the security measures implemented to protect such data and retention of Personal Data by the Bank.

6. DEFINITIONS

The concept of "**Personal Data**" consists of any information, of any nature, regardless of the respective format, including sound and image, relating to any identified or identifiable natural person. Anyone who may directly or indirectly be identified, namely by reference to an identification number or to one or more specific elements of his physical, psychologic, psychic, economic, cultural or social identity, shall be deemed an identifiable person.

This Regulation contains information and the rules for the processing of Personal Data of the following:

- **Clients**, which means natural persons, legal entities or unincorporated organisations:
 - i) to whom the Bank provides services within the scope of its operations ("**Products**") or which provide services for the Bank; or
 - ii) with whom the Bank conducts negotiations, discussions or in relation to which the Bank undertakes any other actions aimed at establishing cooperation with respect to the services provided by the Bank or the entity;
 - iii) in relation to which the Bank takes legal or factual actions in connection with the provision or intent to provide services to the persons indicated in points (i) and (ii), or with the intent, respectively, to make, conclude and execute transactions, ventures, contracts, or services.

- **Related Parties** means natural persons related to the Client, including in particular employees, co-workers, proxies, statutory representatives, members of management or supervisory bodies of legal persons or organisational units without legal personality, partners and shareholders of companies (if they are natural persons) whose personal data is processed by the Bank in connection with activities undertaken with respect to the Clients.
- **Service providers;**
- Members of **Staff**;
- Any other **third parties establishing a relationship** with the Bank;

All of the above are defined as “**Data Subjects**”.

7. PERSONAL DATA

In the context of the relationship established with the Data Subject, the Bank may collect various Personal Data, such as:

| Types of Personal Data | Examples |
|---------------------------------------|--|
| Identification data | Names; nickname; gender; date of birth/age; marital status; Social Security number; passport number; other identification numbers issued by governmental authorities (taxpayer number, visa number or driving licence number); nationality; images of passports, signatures; authentication passwords (passwords, questions and answers, PINs); pictures and images; copies of identification documents; voice and other biometric data. |
| Family data | Names and contact details of family members and dependents. |
| Professional details | Industry, position, business activities, names of current and former employers, work address, work telephone number, email address and work-related profiles on social media. |
| Educational profile | Includes details on your education and qualifications. |
| Financial data | Tax address, bank account numbers, credit card numbers, name of the cardholder or accountholder and their details, records of orders, transaction details, investor profile details and counterparty details. |
| Electronic identification data | Automatically recorded Personal Data such as IP addresses, cookies and electronic identifiers. |

8. CATEGORIES OF PERSONAL DATA

The main categories of Personal Data processed by the Bank are:

| | |
|-------------------------|---|
| Usage data | <p>Usage data may include identification data, electronic identification data, geographic location, operating system, browsing patterns on the website/application and information on the time, frequency and pattern of usage of the service.</p> <p>These usage data may be processed to analyse the use of the website and services.</p> <ul style="list-style-type: none"> ➤ The ground for this processing is the Data Subject's consent. |
| Account data | <p>Account data may include any personal information requested during the client onboarding process.</p> <p>These data may be processed:</p> <ul style="list-style-type: none"> • to establish a business relationship; • to provide services; • to ensure the security of the website/application and services; • to keep backups of the Bank's databases; • to communicate with the Data Subject and comply with the applicable laws and regulations. <ul style="list-style-type: none"> ➤ The ground for this processing may be (i) the performance of a contract; (ii) compliance with legal obligations; or (ii) the Data Subject's consent. |
| Service data | <p>Service data may include identification data, family data, and educational profiles.</p> <p>These service data may be processed:</p> <ul style="list-style-type: none"> • to establish a business relationship; • to provide services; • to ensure the security of the website/application and services; • to keep backups of the Bank's databases; • to communicate with the Data Subject and comply with the applicable laws and regulations. <ul style="list-style-type: none"> ➤ The ground for this processing is (i) the Data Subject's consent; (ii) the performance of a contract; or (iii) compliance with legal obligations. |
| Transaction data | <p>Transaction data may include:</p> <ul style="list-style-type: none"> • the Data Subject's contact details, as well as the transaction details as such, with a view to ensuring compliance with the legal requirements imposed under the applicable law. <p>Transaction data may be processed:</p> <ul style="list-style-type: none"> • to acquire goods and services and duly record these transactions; • to ensure the security of the website/application and services; • to keep backups of the Bank's databases. |

| | |
|----------------------------|---|
| | <ul style="list-style-type: none"> ➤ The ground for this processing may be (i) the Data Subject's consent or (ii) compliance with legal obligations. |
| Notification data | <p>The Bank may process information supplied to subscribe to newsletters and/or notifications by email.</p> <p>Notification data may be processed:</p> <ul style="list-style-type: none"> • to send relevant notifications and/or newsletters; • to ensure the security of the website/application and services; • to keep backups of the Bank's databases. <ul style="list-style-type: none"> ➤ The ground for this processing is (i) the Data Subject's consent or (ii) the performance of a contract. |
| Correspondence data | <p>Correspondence data may include the content of communications and data associated with such communications.</p> <p>Correspondence data may be processed:</p> <ul style="list-style-type: none"> • to communicate with the Data Subject and keep records in accordance with the applicable laws; • to ensure the security of the website/application and services; • to keep backups of the Bank's databases. <ul style="list-style-type: none"> ➤ The ground for this processing is compliance with legal obligations. |

9. PROCESSING OF PERSONAL DATA

The processing of Personal Data consists of any operation or set of operations that the Bank performs on Personal Data, whether by manual or automated means, such as collection, recording, organisation, use, storage, copy and transfer.

The main grounds for the collection of Personal Data by the Bank are:

- compliance with legal obligations;
- the contractual relationship between the Data Subject and the Bank and any action resulting from this relationship.

In order to meet the aforementioned grounds, and assuming that it has obtained the Data Subject's due consent, where necessary, the Bank may process the Data Subject's Personal Data under the following circumstances:

| | |
|-------------------------|--|
| Onboarding | There are legal and regulatory obligations, as well as internal procedures, regulations and policies, that require the Bank to process Personal Data when it deals with the onboarding of clients (for example upon " <i>registration of the user</i> " on the application or website and the onboarding process). |
| AML (anti-money) | In order to comply with the legal and regulatory obligations – including verifications in the context of the Know Your Client ("KYC") procedures – the Bank has to |

| | |
|----------------------------------|--|
| laundering) / KYC | confirm and verify the identity of the client, compare the client database with lists issued by the government, supranational organisations and other agencies, as well as comply with other legal restrictions. |
| Financial due diligence | The Bank may process clients' Personal Data in the context of financial due diligence actions. |
| Services and products | In the context of communications between the Bank and clients and/or counterparties, notably to supply products and services, the Bank may process Personal Data. Accordingly, the Bank may manage the business relationships and related services and may also perform any action necessary to provide and supply the goods and services required. |
| Marketing | The Bank may use Personal Data to communicate with Data Subjects by any means, including email, telephone, mobile messages or social media, ensuring that these communications with Data Subjects are effected pursuant to the applicable law. |
| IT operations | The Bank may process Personal Data in order to ensure and maintain the security of the IT systems that support the Bank's communication and management systems. |
| Financial management | Personal Data concerning sales, finance, corporate audit and management of suppliers are processed so that the Bank may ensure the proper operation of the Data Subjects' financial matters. |
| Research | To carry out market research and client satisfaction surveys, as well as to interact with the client and/or counterparty in order to obtain his or her opinions and points of view with regard to the Bank's services and products. |
| Security | Physical security in the Bank's premises, including registration of visitors and video surveillance recordings, as well as electronic security, which may include recordings of logins and access details when the Bank's electronic systems are used. |
| Forensics | To detect, investigate and prevent offences and infringements of the Bank's Privacy Regulation, pursuant to the applicable law. |
| Compliance and procedures | To comply with regulatory and legal obligations, pursuant to the laws in force and the exercise of rights. |
| Risk management | To carry out compliance and audit controls, as well as for other risk management purposes. |
| Prevention of fraud | To detect, prevent and investigate potentially fraudulent actions. |

a. How Personal Data is processed by the Bank

Personal Data is always collected and processed in full compliance with the applicable legislation. Under no circumstances shall the Personal Data collected be used for any purpose other than that for which it was collected or consented, without prejudice to any processing required or necessary to comply with any laws and regulations applicable to the Bank or the Data Subject.

Personal Data may be collected from various sources, such as:

- when supplied by direct contact, email, telephone, registration on the website or the application or other means of communication;
- in the normal course of the relationship between the Bank and the Data Subjects;
- when the collection of Personal Data is done publicly, which includes information published on social media;
- when the Bank and Data Subjects are subject to any applicable law or regulation that requires the collection of Personal Data;
- when Personal Data is received from duly authorised third parties (collaborators, counterparties, credit rating agencies, law enforcement authorities);
- through cookies: a cookie is a small file that is stored in the device used when Data Subjects browse the Bank's website. Cookies record information on the device, browser and, in certain cases, browsing preferences and habits.

b. Disclosure of Personal Data by the Bank

The Bank may disclose Personal Data to any member of its group of companies, provided that it is reasonably necessary and pursuant to the applicable legislation.

The Bank may further disclose Personal Data to:

- insurance companies and/or professional consultants: provided that it is reasonably necessary to obtain or maintain any insurance cover, manage risks, obtain professional advice, or establish, exercise or defend legal claims, either in court cases or administrative or out-of-court proceedings;
- suppliers of payment and other services, such as IT services: entities that manage transactions related to the Bank's activities (without prejudice to the laws and regulations applicable to payment services which may occasionally require the Bank to disclose Personal Data to an authorised third party). Only data strictly necessary to process payments, refund payments and manage claims and matters related to payments and refunds will be processed.

c. Transfer to third countries (outside the European Union)

Due to the international nature of the Bank's activities, it may be necessary to transfer Personal Data within the Haitong Group and to third parties (outside the European Union).

Transfers of Personal Data to third countries will only be effected strictly in compliance with the applicable legal provisions.

d. Protection of Personal Data by the Bank

The Bank has implemented technical and organisational security measures to protect Personal Data against destruction, loss, modification, non-authorised disclosure or non-authorised access (either accidental or unlawful), as well as any form of unlawful or accidental processing of these data, in accordance with the applicable legislation.

The Bank will do anything necessary to ensure that Personal Data is properly processed and updated whenever necessary.

Should any Personal Data not be accurate (in the context of the purposes for which they are being processed), the Bank will promptly erase or rectify them.

From time to time, and in line with the legal and regulatory requirements, the Bank may ask the Data Subject to confirm whether his or her Personal Data is up to date.

Data Subjects are responsible for ensuring that their Personal Data is sent to the Bank in a secure manner.

e. Storage of Personal Data

Without prejudice to compliance with legal obligations, which may require longer periods of storage, the Bank will take the measures necessary to ensure that Personal Data is processed for the minimum period of time necessary to meet the purposes set.

The criteria for determining the duration for which the Bank will retain the Data Subject's Personal Data are as follows:

- (i) The Bank will retain copies of the Data Subject's Personal Data for as long as: the Bank maintains an ongoing relationship with the Data Subject (e.g., when the Data Subject is a recipient of the Bank's services, or the Data Subject is lawfully included in mailing lists and has not unsubscribed); or the Personal Data is necessary in connection with the lawful purposes set out in this Regulation or any applicable law or regulation (e.g., where Personal Data is included in a contract between the Bank

and the Data Subject employer, and fulfilling obligations under that contract; or when the Bank has a legal obligation to retain the Data Subject Personal Data);

- (ii) After the termination of the business relationship between the Bank and the Data Subject, the Bank shall retain the required Personal Data for the purposes set out under the applicable laws and regulations. Furthermore, the Bank shall also retain for the legally admissible period, at its sole discretion based on a risk approach method, the Personal Data and other elements pertaining to the prior business relationship with the former Data Subject for the safeguard of any claims, legal or regulatory procedures that may be addressed at the Bank, or that the Bank may address to the former Data Subject or any related third-party.
- (iii) Additionally, if any relevant claims, legal or regulatory procedures are brought, the Bank may continue to process the Data Subject Personal Data for additional periods as necessary in connection with such procedures.

Accordingly, Personal Data will be stored in line with their purpose, their storage ending when the ground that supported their purpose ceases.

Thus, upon the purposes of the conservation of data ceasing, the Bank will:

- use its best efforts to permanently erase or destroy the Personal Data;
- file the Data Subject's Personal Data so that they may not be used; or
- anonymise the relevant Personal Data.

The criteria for determining the period of conservation of Personal Data are outlined in our Data Conservation Regulation.

f. Data Accuracy and Minimization

The Bank shall take reasonable steps to ensure that the Data Subject's Personal Data is processed accurately and, when necessary, kept up to date. If any of the Data Subject's Personal Data is inaccurate (for the purposes for which it is processed), the Bank shall erase it or rectify it without delay.

Periodically, and in accordance with legal and regulatory requirements, the Bank may ask the Data Subject to confirm the accuracy of his Personal Data.

The Bank takes the necessary measures to ensure that Data Subject Personal Data processing is limited to the reasonably required in connection with the purposes set out in this Regulation.

10. DATA SUBJECTS' LEGAL RIGHTS

According to the applicable laws and regulations, the Data Subject has a number of rights regarding the processing of Personal Data, including:

| | |
|--------------------------------------|---|
| <p>Right of access</p> | <p>The Data Subject has the right to obtain confirmation from the Bank as to whether or not personal data concerning him or her are being processed, and, where this is the case, access to the Personal Data and certain additional information. This additional information may include:</p> <ul style="list-style-type: none"> i) details on the purposes of the processing; ii) categories of personal data; iii) addressees or recipients that have or may have access to these Personal Data; iv) when possible, the envisaged period for which the Personal Data will be stored. <p>Provided that the rights of third parties are not affected, the Bank shall provide a copy of the Personal Data if requested by the Data Subjects.</p> |
| <p>Right to rectification</p> | <p>The Data Subject has the right to rectify his or her Personal Data that is inaccurate and, taking into account the purposes of the processing, complete any missing Personal Data.</p> |
| <p>Right to erasure</p> | <p>Notwithstanding the exceptions below, the Data Subject has the right to obtain from the Bank the <u>erasure</u> of his or her Personal Data without undue delay.</p> <p>These circumstances include, without limitation, the following:</p> <ul style="list-style-type: none"> i) the Personal Data is no longer necessary in relation to the purposes for which they were collected and subsequently processed; ii) the Data Subject withdraws his or her consent, on which the processing of his or her Personal Data is based; iii) the Data Subject objects to the processing of Personal Data under certain applicable data protection rules; iv) the processing is for direct marketing purposes; and v) the Personal Data has been unlawfully processed. <p>However, there are <u>some exclusions from the right to erasure</u>, notably:</p> <ul style="list-style-type: none"> • when the processing and conservation of the Personal Data in question is necessary to exercise the Bank's rights; • to comply with legal obligations; or • for the establishment, exercise or defence of legal claims. |

| | |
|--|--|
| Right to restriction of processing | <p>Under certain circumstances, the Data Subject has the right to restrict the processing of his or her Personal Data.</p> <p>These circumstances are:</p> <ul style="list-style-type: none"> i) the Data Subject contests the accuracy of the Personal Data; ii) the processing is unlawful, but the Data Subject opposes the erasure of his or her Personal Data; iii) the Bank no longer needs to process the Personal Data, but the Data Subject requests that they be made available for the purposes of being able to establish, exercise and defend legal claims; iv) the Data Subject has objected to the processing of his or her Personal Data, pending verification of his or her objection. |
| Right to object | <p>The Data Subject has the right to object to the processing of Personal Data based on special circumstances, which may include:</p> <ul style="list-style-type: none"> i) processing for direct marketing purposes (including profiling for direct marketing); ii) for scientific or historical research purposes or statistical purposes on grounds relating to his or her particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest. <p>However, the objection shall be restricted to the cases when the processing of Personal Data by the Bank is necessary, such as:</p> <ul style="list-style-type: none"> i) the performance of a task carried out for reasons of public interest; ii) the exercise of any official power granted to the Bank; iii) the pursuit of the Bank's or third-party's lawful interests. |
| Right to data portability | <p>The Data Subject has the right to receive his or her Personal Data, which he or she has provided to the Bank, in a structured, commonly used and machine-readable format and has the right to transmit that data to another controller.</p> |
| Right to lodge a complaint with a supervisory authority | <p>The Data Subject has the right to lodge complaints with the competent supervisory authorities in respect of matters related to the exercise of his or her rights.</p> |
| Right to withdraw consent | <p>Data Subjects may withdraw their consent at any time.</p> |

11. ARCHIVE

- a. The Compliance Department maintains an archive in digital format of this Regulation. This digital archive is maintained in the Compliance Department's shared folder "Comply".

12. MONITORING

- a. The Compliance Department monitors compliance with this Regulation by centralising the requests from Data Subjects and ensuring that they are properly addressed.
- b. The Compliance Department provides regular training to the staff of the Bank regarding this Regulation and the regulatory rules concerning transactions with Related Parties.
- c. Any failure to comply with the duties set out in this Regulation is a serious breach of the legal and contractual duties of the Bank's staff.
- d. The Compliance Department coordinates with the Administrative Department this Regulation on the Bank's intranet and website.

13.CONTROL OF VERSIONS

Table 1: Information about the Document

| | |
|---------------------------------|--|
| Name of the Document | Personal Data Privacy Regulation Regulation |
| Version | 3.0 |
| Prepared by (Name/Department) | Compliance Department |
| Appreciated on (Committee name) | NA |
| Approved by (Committee name) | Board of Directors |

Table 2: Versions' update

| Update and Approval Date | Main Changes |
|--------------------------|--|
| Version 1.0 - 20/01/2020 | First draft of the Regulation further to entering into force of GDPR |
| Version 2.0 - 15/09/2020 | Ratification by the Board of Directors |
| Version 3.0 - 19/12/2022 | Modification of the structure of to the Regulation. Clarification of certain points, particularly with regard to the chapters "Processing personal data" and "Transfer to third countries (outside the European Union)". |