PRIVACY POLICY

1. GENERAL

The purpose of this Privacy Policy is to explain, in a simple and transparent way, how the Bank processes (in particular collects, uses, and safeguards) personal data of natural persons in the course of the business activities. “Processing” includes any activity with a personal data which is provided to the Bank. Personal data includes any information relating to an identified or identifiable a natural person.

In its capacity as a **Data Controller**, the Bank is committed to ensure compliance with the applicable personal data protection rules when carrying out its business activities.

1.1.Glossary

Bank - Bank GPB International S.A. is authorised as a credit institution and is under the prudential supervision of the Luxembourg supervisory authority, the Commission de Surveillance du Secteur Financier (the “CSSF”), and registered in the Luxembourg Trade and Companies Register (R.C.S. Luxembourg) under number B178974. The registered and business address of the Bank is at 31 avenue Monterey L-2163 Luxembourg City, the Grand Duchy of Luxembourg.

Personal data - Any information relating to an identified or identifiable natural person (the data subject) within the meaning of the General Data Protection Regulation (**GDPR)**. An **identifiable natural person** is deemed to be an individual who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data or an online identifier, or by reference to one or more factors specific to their physical, physiological, genetic, psychological, economic, cultural or social identity.

Data subject - Individual whose personal data is processed by the Bank.

1.2. Scope

This Privacy Policy applies to the following individual persons (**categories of Data subjects**):

- current, former and protentional clients who express an interest in the Bank’s products and services;
- any individuals involved in any transaction with the Bank;
- counterparties of the Bank;
- agents, representative or other affiliates of our clients (e.g. family members/prospects);
- persons acting on behalf of corporate clients, including legal representatives, managers, directors, administrators, employees, attorneys and authorized signatories;
- beneficial owners and shareholders of a client company;
- job applicants as part of the recruitment process;
- heirs, attorneys or any other person acting in the name and on behalf of the Bank’s clients;

- users of the Bank’s websites and mobile applications;
- visitors of the Bank’s premises;
- any other individuals in contact with the Bank.

1.3. Source of Personal Data

The Bank may obtain the personal data in the following way:

Directly from the Data subject, for example when opening an account, performing a transaction, or making contact (email, letter, telephone, etc.).

I**ndirectly from external public sources**. In some cases (e.g. the Bank anti-money-laundering screening, sanctions monitoring), the Bank may collect and process information about individuals from external sources without informing them individually, when this is required by law.

At that rate, the Bank can use the public registers such as e.g. the Trade and Companies Register, or the Register of Beneficial Owners, Internet, world press, news, and other publicly available media, specialized AML/CTF and security service providers and/or legitimately provided by other member of the Bank’s group, when working on group-related matters or clients.

From third parties. If an individual or an organization in direct contact with the Bank provides personal data of third parties (e.g. family members, attorneys, beneficial owners, etc.), they are responsible for ensuring that those individuals are properly informed about such disclosure and the possible processing of their data by the Bank and to direct them to this Policy.

2. CATEGORIES OF PERSONAL DATA

The personal data which the Bank processes may include the following information and documents on the Client and, where applicable, the Client’s representatives, agents, officers, related parties, transaction counterparties and beneficial owners and other individuals related to the Client relationship:

2.1 Identification and contract information:

- full name, alias (if any), gender, the date and place of birth, nationality, photo, signature;
- residential address, email address, phone number(s);
- data relating to education and employment (such as data relating to level of education, occupation, position, name of employer, remuneration, exercise of a public/political function);
- data relating to family situation (such as marital status, matrimonial property regime, number and age of children, household composition).

2.2 **Identity documentational data:**

- identification documents type (national/passport/ID card) number, date and place of issue, expiry date, and issuing authority;
- copies of identity documents;

2.3 **Financial and account related data:**

- bank account numbers, account balances, and transactions history on accounts;
- source of funds, purpose of the transactions, and other financial information relevant to the Bank's services;

2.4 **KYC and verification data:**

- images or scans of ID cards and other documents used for identity verifications;
- information gathered for AML/CFT compliance checks;
- data on criminal convictions, offences, penalties and negative/unfavorable media coverage.

2.5 **Tax and regulatory data:**

- economic, financial/asset and tax data (such as tax identification number, tax status, country of residence for tax purposes, remuneration and other income, financial situation, statement of assets);
- relevant documentations related to tax status and obligations.

2.6 **Surveillance and communication data:**

- data recorded by video surveillance cameras (such as images, date, place and time recorded by surveillance cameras. Data subjects are informed of this by means of signs and pictograms in areas where video surveillance is in use);
- recording of certain telephone conversations (where required by law and especially MIFIDII for recording of client orders over the phone. Reference to recording of communications with the Bank is described in the Bank's General Terms and Conditions published on the Bank's website);
- email communication.

2.7 **Digital identifiers and access data:**

- electronic identification data (e.g., email, IP, Bloomberg addresses and other similar identifiers;

- electronic signature (such as the signature itself and the contact data associated with this signature, in particular, the first name, last name, and business email address of the signatory), etc.).

2.8 **Investment and financial suitability information:**

- the Client's investment objectives, risk tolerance, financial situation, knowledge and experience in investment matters and responses to suitability questions;
- the data with respect to the Client's financial status (e.g., salary, assets, liabilities, expenses, income, wealth).

2.9 **Counterparty and transaction data:**

- details of counterparties and third parties involved in transactions executed by or on behalf of the Client, including contracts and terms of financial instruments or services.

2.10 **Other data:**

Any other personal data the Bank may receive and collect in the context of the Client or Counterparty relationship, as required to comply with legal obligations or to provide banking and financial services.

3. LEGAL BASES AND THE PURPOSES OF PERSONAL DATA PROCESSING

The processing carried out by the Bank is based on the legal grounds set out in the GDPR and is always linked to specific purposes. The Bank processes personal data to provide and manage services for the Client, to comply with legal and regulatory obligations, and to pursue its legitimate interests as a regulated credit institution.

3.1. **Performing of a contract.**

The Bank processes personal data where this is necessary to:

- perform banking transactions requested by the Client;
- implement, administer and manage the contractual relationship with the Client and deal with any related matters;
- in the context of asset-backed, commodity or other similar financing, track or otherwise monitor the relevant assets of the Client;
- handle any dispute resolution, complaints and litigation matters.

3.2. Compliance with legal obligation.

The Bank processes personal data where this is necessary to:

- comply with laws and regulations, acts, decisions, recommendations or inquiries of the courts, regulators and other competent authorities;
- comply with banking, tax and anti-money laundering, counter-terrorist financing, sanctions, crime prevention, fraud prevention, market abuse and other similar matters;
- Respond to and comply with requests from local or foreign authorities (including in relation to conflicts of interest, payment services, markets in financial instruments (MiFID), whistleblowing, harassment, market abuse, tax matters, etc.);
- conduct pre-contractual KYC checks on the Client;
- record telephone conversations where required by law (in particular MiFID II requirements for recording order-related communications).

3.3. Legitimate interests of the Bank.

The Bank processes personal data where this is necessary for its legitimate interests, provided that such interests are not overridden by the rights and freedoms of Data subjects. These legitimate interests are linked to the functioning and development of the Bank as a regulated credit institution and may include:

- building up or expanding relationship with the Client;
- marketing and research activities (including statistical and analytical work on the Bank's client base and preferences);
- management of the Bank's IT infrastructure (including the security of information systems, encryption and decryption of Client-related information);
- internal management and control (including, any reporting, business analysis, business controls, audits, investigations and risk management);
- exchange of information between the Bank and other members of the Group where required for risk management, consolidated supervision or group level services (in some cases also based on legal obligations);
- operation and improvement of Bank's website and online services;
- various matters related to human resources management (where based on legitimate interests rather than other legal basis);
- any other matters where the processing of personal data is necessary or desirable to ensure the on-going provision of banking services to the Client, the status of the Bank's status as a regulated credit institution.

3.4. Consent.

In limited situations, mainly in connection with human resources activities and certain features of the Bank's website or online services, the Bank may rely on the Data subject consent as a legal basis for processing.

Where the Bank relies on consent:

- the data subject will be clearly informed that consent is the legal basis for the processing;
- the data subject may withdraw their consent at any time by a contacting the DPO or their usual contact at the Bank;
- Withdrawing consent does not affect the lawfulness of processing carried out before the withdrawal.

4. THIRD-PARTIES' PERSONAL DATA

The Client shall inform all relevant natural persons related to the Client (such as agents, delegates, managers, employees, attorneys, service providers, shareholders or beneficial owners and any other related individuals) about the contents of this Privacy Policy.

By providing personal data of such individuals to the Bank, the Client confirms that those individuals have been properly informed that their personal data may be disclosed to, and processed by, the bank in accordance with this Privacy Policy.

5. USE OF PROCESSORS AND EXTERNAL SOURCES

For its Clients and counterparties, the Bank is required to perform regular KYC, KYT and other similar back-ground checks. For these proposes, the Bank may:

- use specialised service providers and external databases;
- consult publicly available information (such as official registers, press and the Internet).

The Bank may obtain and process information in this way without further individual notice or additional consent, where such processing is based on legal obligations or the legitimate interests of the Bank.

Where the Bank uses external service providers to process personal data on its behalf, such entities act as data processors and are bound by contractual obligations to:

- process personal data only on the Bank's documented instructions; and
- implement appropriate technical and organizational measures to protect personal data.

6. PROFILING AND AUTOMATED DECISION-MAKING

Certain regulatory requirements (e.g., assessment of the suitability or appropriateness of financial instruments for the Client) may require the use of scoring systems or similar tools.

However:

- decisions with significant impact on the Client are not taken solely on the basis of automated processing;
- a Bank officer is involved in reviewing and conforming such decisions.

The Client may always contact their relationship manager to request explanations regarding any decisions taken in relation to them and to contest such decisions if they disagree.

7. RECIPIENTS OF PERSONAL DATA

The Client's personal data may be disclosed or transferred by the Bank, without further specific notice or additional consent of the Client, to following categories of recipients:

7.1. Public authorities and bodies:

- where required by applicable law or court order;
- pursuant to the rules or regulations of any government, supervisory, stock-exchange, tax or regulatory body;
- in connection with legal or arbitration proceedings, investigations or regulatory inquiries.

7.2. Group to which the Bank belongs:

entities within the Bank's Group for purposes such as a risk management, consolidated supervision, group reporting, internal control and support functions, where permitted by law.

7.3. Service providers and professional advisers:

- officers, directors, employees of the Bank and its affiliates;
- auditors, lawyers and other professional advisers;
- other financial institutions, payment services providers, issuance companies, card issuers, issuing agents and correspondent banks;
- IT and telecommunication companies, outsourcing providers, data centers and cloud provider;
- other vendors and subcontractors involved in providing services to the bank or its affiliates.

7.4. Corporate transaction:

- in connection with any corporate reorganisation, restructuring, merger, transfer of business or similar transaction involving the Bank.

7.5. Other third parties:

- any third parties to whom the Bank or its affiliates reasonably consider it necessary or desirable to disclose personal data for the performance of their duties, obligations or activities, whether arising from a contract, legal obligation or legitimate interest.

In particular, the Bank outsources the IT processing of its financial operations to a third-party provider and retains its right to change such service provider at any time without further notice to, or consent of, the Client.

Any transfer of personal data outside the European Union (EU) / the European Economic Area (EEA) will be carried out with appropriate safeguards, as required by Luxembourg law and the GDPR.

8. SECURITY

The Bank has implemented and requires its processors to implement, appropriate technical, physical and organisational measures to protect personal data against:

- accidental or unlawful destruction or accidental loss;
- unauthorised access, alteration or disclosure;
- any other unlawful forms of processing.

These measures are designed taking into account the state of the art, implementation coast, the nature of the data and the risks for the rights and freedoms of individuals.

9. RETENTION PERIODS

The Bank retains personal data only foe as long as necessary for the purposes for which the data were collected and to comply with applicable legal, regulatory and contractual obligations.

In general:

- most of the personal data relating to the Client and their transactions are retained for up to 10 years following the end of the business relationship;
- employees’ and job applicants’ data are retained for at least the minimum periods aet out in employment and social security laws and, where applicable, for longer if required for the establishment, exercise or defense of legal claims.

Where a shorter or longer retention period is required by law, regulation or supervisory guidance, the Bank will apply the period required by such rules.

10. CROSS-BORDER TRANSFERS

Where the Bank transfers personal data outside the European Union (EU) / European Economic Area (EEA), such transfers are made only:

- to jurisdictions that have been recognized by the European Commission as providing an adequate level of data protection; or
- on the basis of appropriate safeguards in accordance with Chapter V of the GDPR, such as Standard Contractual Clauses, Building Corporate Rules, or other transfer mechanisms permitted under the GDPR.

Before relying on such transfer mechanisms, the Bank performs an assessment of the legal and regulatory environment of the destination country and implements supplementary measures where necessary.

11. COOKIES ON THE BANK'S WEBSITE

Cookies are small files placed on your device when you access the Bank’s websites (e.g. the Bank’s main website or online banking portal.) They store certain information about your visit.

The Bank uses only the following types of cookies:

Strictly necessary cookies – these are required for the technical functioning and security of the website and to enable core features (e.g., page navigation, secure access). Without these necessary cookies the website cannot function properly. For this reason, strictly necessary cookies cannot be disabled.

Limited analytics cookies – these help the Bank understand, in an aggregated way, where visitors come from and which products or pages, they are interested in. This allows the Bank to improve its website and services. The information collected does not directly identify individual visitors. You can disable these cookies at any time using your browser settings.

For more information on cookies or how to manage it, please contact the Bank at the following email **DPO@gazprombank.lu.**

12. BANK’S E-BANKING AUTHENTICATION APPLICATION

The Bank’s E-Banking authentication Application:

- is used purely for authentication purposes; and

- does not collect personal data beyond what is technically necessary for authentication and security.

With respect to the information regarding any transactions which the Client instructs through the E-Banking authentication Application, the standard retention period set out in Section 9 (Retention Periods) applies.

13. DATA SUBJECT RIGHTS

13.1 Data subject have the following rights in relation to their personal data:

- **Right to be informed** about how the Bank processes their personal data;
- **Right of access** to their personal data held by the Bank;
- **Right to rectification** of inaccurate or incomplete personal data;
- **Right to restriction of processing** in the circumstances provided by law;
- **Right to object** to certain types of processing, including direct marketing;
- **Right of portability**, where applicable;
- **Right to erasure** of personal data (so-called **right to be forgotten**).

13.2. The exercise of the above rights may be subject to legal restrictions. Where a data subject submits a request, the Bank will assess it in light of the applicable rules and provide a reasoned response.

In exceptional cases permitted by law, the Bank may charge a reasonable fee.

13.3. To exercise any of these rights, the Data subject may complete the form attached to this Privacy Policy and send it:

- to their relationship manager using any authorised method of communication; or
- to the Data Protection Policy by email to DPO@gazprombank.lu; or
- by post to BANK GPB INTERNATIONAL S.A., 31, Avenue Monterey, L-2163 Luxembourg, Atten.: DPO.

Please indicate in the subject line "Data Protection Officer – Exercise of Data Subject Rights Request" and attach a copy of your valid ID.

Before responding to any data protection request, the Bank will first take reasonable steps to verify the identity of the requester. Once the identity has been confirmed, the Bank will provide a response without undue delay and, if any event, within one month from the date of receipt of the verified request. This period may be extended by up to two additional months where necessary, taking into account the complexity and number of requests. In such cases, the Bank will inform the requester of any extension and reasons for it.

13.4. If the Client or any other data subject is not satisfied with the Bank's response, they may lodge a complaint with the Luxembourg National Commission for Data Protection (La Commission nationale pour la protection des données - CNPD).

Commission nationale pour la protection des données

15, Boulevard du Jazz

L-4370 Belvaux, Luxembourg

Luxembourg

Telephone: (+352) 26 10 60 -1

Complaint form IS available on its website: https://cnpd.public.lu

14. UPDATING OF THE POLICY

This Policy may be amended at any time to comply with legal and regulatory developments or to respond to changes in the Bank’s activities.

You can read the latest version of this document on the Bank’s Website.

Data of publication: __ December 2025

Form of Request

Date:	
GENERAL INFORMATION:	
Full name (including patronymic, maiden names, etc.):	
Date of birth:	
Full resident address:	
Telephone:	
Email:	
YOU ARE (please select):	A client of Bank GPB International SA and my IBAN is ________________________________
	Other and my relationship with Bank GPB International SA is as follows:
PROVIDED ID:	Please state the full name of the provided ID document and issue details:
THE RIGHTS YOU WANT TO EXERCISE:	Please indicate which rights you want to exercise (e.g., the right to access, rectify or erase data, the right to restrict its processing, the right to object, or the right to data portability):
SIGNATURE:	