Annex 2 Data Privacy Policy

Banque de Luxembourg, a Luxembourg société anonyme (public limited company) with its registered office at 14, boulevard Royal, L-2449 Luxembourg and registered in the Luxembourg Trade and Companies Register (R.C.S. Luxembourg) under number B5310 (hereinafter, the "Bank" or "we"), processes personal data in the course of its business activities. In its capacity as Data Controller, the Bank ensures compliance with the rules on the protection of personal data in order to build or maintain relationships with data subjects based on transparency and trust.

To this end, the Bank takes the necessary measures to meet its obligations and pays particular attention to the security of the personal data it processes, as it wants people to feel safe when they use the Bank's services.

The Bank has drawn up this Policy as well as cookie management policies which, together with all the other documents referred to in this Policy, are intended to inform data subjects in a transparent manner about the processing of personal data that may be implemented depending on the situation of the data subject and their relationship with the Bank.

This Policy, in conjunction with our cookie management policies, are available on the Bank's Website in the section entitled "PERSONAL DATA PROTECTION" as well as the section entitled "COOKIE CONSENT MANAGEMENT".

1. Glossary

"Bank": Banque de Luxembourg, a Luxembourg société anonyme (public limited company) with its registered office at 14, boulevard Royal, L-2449 Luxembourg and registered in the Luxembourg Trade and Companies Register (R.C.S. Luxembourg) under number B5310.

"Personal data": Personal data within the meaning of the GDPR: any information relating to an identified or identifiable natural person (the data subject).

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.

"Online banking": Electronic service offered by the Bank enabling clients to have Internet access to their account(s) via the Bank's private online website or its mobile application (hereinafter the "E-Banking Services").

"DPO": Data Protection Officer.

"Data subject": Individual whose personal data is processed by the Bank, in particular clients, their relatives, prospective clients of the Bank, users of the Website, mobile application and banking applications provided by the Bank, suppliers and visitors to the Bank's premises.

This Policy does not apply to employees of the Bank, directors of the Bank, candidates for employment as part of the Bank's recruitment process, or employees, representatives or contact persons of the Bank's external service providers and subcontractors.

"Policy": This personal data protection policy.

"The Bank's service provider": Any external supplier of the Bank, regardless of their role as independent personal data controller, joint controller or processor within the meaning of the GDPR.

"Profiling": Any form of automated processing of personal data involving the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict factors concerning this individual's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

"Automated individual decision-making": any operation or set of operations carried out using automated processes and applied to personal data or sets of personal data.

"Controller within the meaning of the GDPR": The natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing; where the purposes and means of such processing are determined by EU law or by the law of a Member State, the controller may be designated or the specific criteria applicable to their designation may be laid down by EU law or by the law of a Member State.

The Controller in this case is the Bank.

"GDPR or General Data Protection Regulation": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Website": The Bank's public website: https://www.banquedeluxembourg.com.

"Processor within the meaning of the GDPR": The natural or legal person who processes data on behalf of the controller.

"Third party within the meaning of the GDPR": A natural or legal person, public authority, agency or body other than the data subject, the data controller, the processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"Personal data processing within the meaning of the GDPR": Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, extraction, consultation, use, disclosure by transmission, dissemination or any other form of provision, alignment or combination, restriction, erasure or destruction.

"Visitor": Any person other than an internal or external employee, service provider or supplier of the Bank entering the Bank's premises or visiting our Website.

2. Controller and DPO

In the context of its relations with the categories of persons listed in Section 3 of this Policy, the Bank assumes the role of Controller:

Controller:
Banque de Luxembourg
14, boulevard Royal
L-2449 Luxembourg
Telephone: (+352) 49 924-1

Contact details for the DPO:
For any questions you may have about the processing of your personal data by the Bank, or requests relating to the exercise of your rights, please contact the Bank's DPO:

– by email: dpo@blu.bank

– by post:

Banque de Luxembourg
For the attention of the Data Protection Officer
14, boulevard Royal
L-2449 Luxembourg

3. Categories of data subjects

The Bank processes the personal data of individuals with whom it has, had, or is likely to have a direct or indirect relationship (hereinafter, the "data subjects" or "you"):

– clients;

– heirs, attorneys or any other person acting in the name and on behalf of the Bank's clients;

– all persons within a client company, including legal representatives, managers, directors, administrators, employees, attorneys and authorised signatories;

– the beneficial owners and shareholders of a client company;

– principals and/or beneficiaries in relation to transactions carried out by clients;

– prospects or potential clients who express an interest in the Bank's products and services;

– family members of clients/prospects;

– visitors;

– third-party guarantors;

– business introducers. In this context, the Bank reserves the right to identify any physical person referring a new client, and to carry out any appropriate due diligence measures;

– any other individual in contact with the Bank.

The following categories of persons are covered by their own separate information notice:

– employees of the Bank;

– executives and administrators of the Bank;

– job applicants as part of the Bank's recruitment process;

– the employees, representatives and contact persons for the Bank's external service providers and subcontractors.

4. The categories of personal data processed by the Bank

Depending on the purpose pursued by the Bank, the situation of the data subject, and their relationship with the Bank, the Bank may be required to process different categories of personal data. This may include:

– identification data (such as first name and surname, gender, date and place of birth, nationality, photo, signature, national/passport/ID card number, etc.);

– private or business contact data (such as email addresses, postal addresses, telephone number);

– data relating to family situation (such as marital status, matrimonial property regime, number and age of children, household composition);

– data relating to your interests (including but not limited to interest in an activity);

– data relating to personal life (for example, specific dietary requirements);

– 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 the terminal used (computer, tablet, smartphone, etc.) when connecting to the Bank's Website and applications (in particular IP address, operating system, country of connection, etc.), and data relating to habits and preferences (such as data relating to browsing behaviour and preferences as well as data relating to the use of products and services subscribed to with the Bank, etc.). For more information regarding the processing of data, please consult our cookie management policy on our Website, under the heading "Cookie Consent Management";

– 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);

– data contained in the national centralised records that must be consulted by the Bank as part of a credit application (Fichier des incidents de remboursement des crédits aux particuliers – FICP, and Centrale des Crédits aux Particuliers – CCP);

– banking and financial data (such as data relating to bank account number, client number, bank card number, portfolio number, transfers of funds, assets, investor profile, products and services subscribed to, existence of credit with another bank, third-party guarantor at another bank);

– transactional data (such as data on financial transactions, including credit transfers with data relating to the names and addresses of beneficiaries and instructing parties);

– data collected in the context of meetings and other exchanges with you on the Bank's premises, on our Website, our applications, our social media pages, during meetings, telephone calls, video conferences, emails exchanged via Securemail, personal emails not secured by the Bank;

– all paper and electronic correspondence;

– data relating to health (such as data regarding the person's legal capacity to act);

– data on criminal convictions, offences, penalties and negative/unfavourable media coverage;

– 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 (such as audio recording of telephone calls received or made by the Bank or calls made internally within the Bank together with the related data such as the caller's telephone number, the telephone number called, and the date/time and length of the conversation. The persons concerned are informed of these recordings by a message at the start of the call for incoming calls);

– electronic signatures (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).

5. The collection of personal data by the Bank

The Bank may collect the Client's personal data in the following ways:

5.1 Direct collection

– when making contact, regardless of the communication channel (telephone, email, letter, etc.);

– at events, conferences and workshops organised by the Bank;

– upon entering into a business relationship and throughout it;

– when visiting our Website;

– when using one of our applications;

– when you participate in one of our non-anonymous surveys;

– when you use our services;

– when you subscribe to our newsletters;

– when you are filmed by our video surveillance cameras during a visit to our premises and when using one of the Bank's ATMs;

– when you publish your data on social media to which we provide access.

5.2 Indirect collection

– from external sources using public registers (such as the Trade and Companies Register, or the Register of Beneficial Owners, etc.);

– from external sources as part of the Bank's efforts to fight money laundering and terrorist financing;

– from public information such as that published in the press/media;

– from third parties: public authorities and institutions, undertakings operating professional databases, national centralised files, other financial institutions, partners, subcontractors;

– via social networks (Facebook, Instagram, LinkedIn, YouTube, X (formerly Twitter)) to interact with data subjects (public or private messages). The Bank has access to personal data that data subjects make public. The Bank also acts as joint controller with the social networks concerned when it uses the social network logo, "like" or sharing buttons on the Website.

For more information on the processing of personal data on the various social networks, please consult the information notices published on these networks:

Facebook: https://fr-fr.facebook.com/policy.php

Instagram: https://help.instagram.com/519522125107875/?maybe_redirect_pol=0

LinkedIn: https://fr.linkedin.com/legal/privacy-policy

YouTube: https://policies.google.com/privacy

X: https://twitter.com/fr/privacy

When data subjects with whom the Bank is in direct contact transmit the personal data of other persons related to them (family members, attorneys, beneficial owners, etc.), it is the responsibility of the data subjects to request authorisation and to inform the persons in question that the Bank is processing their personal data and to direct them to this Policy.

6. Legal bases and the purposes for which the Bank processes personal data

The processing carried out by the Bank rests on the legal bases provided for in the GDPR and is conducted for specific purposes.

6.1 Processing necessary for the performance of pre-contractual measures/a contract

– managing client relationships (provision and management of services and products, execution and recording of your financial transactions, provision and management of bank cards, granting and management of credit, etc.);

– provision and management of E-Banking Services;

– aggregation of accounts with other banks;

– telephone call recordings, for example in order to verify or provide proof of any business commitment/communication/transaction related to any service provided, business exercised or transaction made by the Bank on behalf of the Client.

6.2 Processing performed on the basis of consent

– commercial prospection, organising events and sending publications to prospects who are natural persons for their own needs;

– management of trackers on the Bank's Website and mobile application.

6.3 Processing performed on the basis of legal obligations

– fighting money laundering and terrorist financing (AML/CFT);

– compliance with requests and requirements from local or foreign authorities (prevention and management of conflicts of interest, payment services and markets in financial instruments (MiFID), whistleblowing, harassment, market abuse, tax regulations, etc.);

– regulatory reporting and automatic exchange of information (DAC, FATCA, CRS, etc.);

– assessment of your creditworthiness and repayment capacity as part of a credit application;

– telephone call recordings in order to comply with MiFID II regulations.

6.4 Processing carried out on the basis of the legitimate interest of the Bank

– organising events and sending publications to the Bank's customers and contacts;

– commercial prospection, organising events and sending publications to individuals as part of their function within a corporate prospect (investment firm, company, etc.);

– commercial prospection of clients on products similar to the contracts subscribed;

– producing studies, analyses, models and statistics (for example, segmentation of Bank clients);

– continuous improvement and personalisation of the Bank's services;

– management of Bank counterparty contacts;

– the recording of telephone calls aimed at improving the quality of the Bank's services;

– traceability of withdrawals from ATMs;

– development and maintenance of online banking services for clients;

– video surveillance for security reasons, to protect people and property, and to manage access to buildings and car parks;

– telephone call management;

– management and prevention of fraud and corruption;

– handling security incidents and events;

– electronic signature to simplify and speed up the contractual commitment and authentication process and, in particular, to prevent fraud.

7. The categories of recipients of personal data

As part of its mission, the Bank may transfer your personal data to the following categories of recipients:

7.1 Sharing internally and within the Group to which the Bank belongs

As part of its contractual, service, legal or regulatory obligations (such as the fight against money laundering or terrorist financing), the Bank may be required to share personal data with other companies in the Crédit Mutuel Alliance Fédérale group to which the Bank belongs (the "Group").

In this context, the Bank: shares such personal data only with departments of Group companies that have a duly justified need.

7.2 Sharing of data outside the Bank and the Group

The Bank shares personal data with its service providers (technical, banking, events, IT, investigators, etc.), lawyers and auditors, where applicable and necessary for the performance of the service.

Accordingly, the Bank provides a framework for the relationship, in particular via:

– a signed contract covering the elements required by the applicable regulations to set out in detail the way in which the service provider may process personal data;

– signing a confidentiality agreement;

– the requirement to implement technical and organisational security measures at least equivalent to those of the Bank.

The Bank shares personal data with its service providers, lawyers and auditors in the following cases:

– In the proper execution, implementation and management of commercial contracts signed with its clients, including:
  – other credit institutions;
  – financial sector professionals such as delegated managers of sub-custodians or central securities depositories;
  – notaries and lawyers;
  – investigators;
  – insurance companies;
  – payment applications;
  – service providers processing bank orders;
  – service providers providing electronic identification of the client for access to the Website;
  – fund promoters, fund managers, fund distributors and any service providers in connection with the funds;
  – service providers performing certain tasks related to the fight against money laundering, terrorist financing, and prevention and management of market abuse, in particular i-Hub S.A.;
– As part of the management of postal correspondence with the Bank's Clients, prospective clients, etc.
– As part of present deliveries with suppliers, transporters or others.
– In the management, control and production of any financial, accounting or regulatory document, including in particular legal declarations to the competent Luxembourg or foreign authorities (for example, transaction reporting obligations under the applicable laws on financial instruments), particularly with service providers assisting it in the production of certain reports.
– As part of the organisation of events with service providers such as restaurants, hotels, carriers, venue managers and videoconferencing applications with whom it works.
– In connection with sending out newsletters and publications, in particular with its service providers for the distribution of the various newsletters and publications.
– In the proper execution, implementation and management of commercial contracts with service providers such as auditors and trustees.
– As part of the maintenance of the Website and applications with technical service providers.
– In the context of access by social media to personal data collected on the Bank's promotional pages.
– Within the framework of legal obligations, the Bank may transmit personal data directly or via service providers to recipients as defined by law.

In certain cases, the authorities require the Bank to share clients' personal data with third parties, such as public authorities, tax authorities, supervisory authorities or legal/investigation authorities or, where applicable, with lawyers, notaries, guardians or auditors.

8. Period for which personal data will be stored

The Bank takes all reasonable steps to ensure that personal data are only processed and stored for the period necessary for the purposes set out in this Policy.

The retention period of your data is variable and depends on the nature of the data and the purposes pursued, to which are added the retention periods imposed by the applicable legal and regulatory provisions.

In general, the Bank will keep your personal data for a period of:

– thirty (30) days maximum for data derived from video surveillance;
– three (3) years from the end of the exchanges between the data subject (e.g. a prospect) and the Bank;
– ten (10) years from the end of the entire contractual relationship when there is a contract that binds the Bank and the data subject.
– ten (10) years from recording for data derived from telephone conversations.

For legitimate reasons and depending on the circumstances, the Bank may retain data beyond the defined period in compliance with applicable legal regulatory provisions.

The Bank has a specific internal policy relating to the retention period for documents and personal data.

9. Transfer of personal data

Given the international scope of the Bank's activities and without prejudice to the legal and regulatory provisions provided for by foreign law applicable in a particular context, personal data may be subject to secure transfer to entities located in countries outside the European Economic Area ("EEA") subject to an adequacy decision issued by the European Commission (Articles 44 and 45 of the GDPR).

In the absence of such a decision, the Bank implements appropriate guarantees to protect your personal data in the context of such transfer (Article 46 of the GDPR).

On the basis of a legal derogation, the Bank may transfer personal data to countries outside the EEA where, for example, the transfer is necessary for the performance of a contract (Article 49 of the GDPR).

10. Automated decision-making including profiling

Within the legal and regulatory limits, processing carried out by the Bank may give rise to automated decision-making, including profiling, for the following purposes in particular:

– securing your transactions;
– fight against fraud and corruption;
– personalisation of the relationship with our clients;
– business development;
– obligations relating to compliance risk management.

11. Subsequent processing of personal data

The Bank does not undertake any subsequent processing of personal data for purposes other than those for which the data was collected.

12. Security of personal data

12.1 Security of personal data

The Bank has drawn up an information security policy that defines objectives, scope, roles and responsibilities, particularly in the area of data security.

Accordingly, the Bank has adopted appropriate measures to protect your personal date with the degree of security proportionate to the level of risk.

These technical and organisational measures are designed to guarantee the confidentiality, integrity and availability of your personal data. In particular:

– risk analyses are carried out before any personal data is processed;

– Bank staff are trained and made aware of personal data protection;

– the recipients of your personal data undertake to implement security measures proportionate to the risk;

– any personal data breach likely to pose a risk to your rights and freedoms is notified to the competent authority;

– any personal data breach likely to cause a high risk to your rights and freedoms will be notified to you as soon as possible.

The measures put in place by the Bank are regularly reviewed and adapted to changes in risk.

The security of your personal data also depends on good practice on your part. In particular, you can consult our Website in the section entitled "SECURITY ON THE INTERNET" in the "HELP AND ASSISTANCE" area (Security on the Internet – Banque de Luxembourg).

12.2 Accuracy of personal data

Data subjects undertake to provide the Bank with accurate personal information upon initial request, to inform the Bank as soon as possible of any change regarding such information and to send the Bank upon simple request any additional information that the Bank may deem useful for maintaining banking relationships and/or that is required by legal or regulatory provisions and in accordance with the principle of personal data minimisation.

The Bank also takes all reasonable steps to ensure that personal data is accurate and kept up to date by allowing data subjects to amend inaccurate personal data at any time and that personal data is collected for the purposes set out in this Policy.

13. Rights of data subjects and how to exercise them

Subject to the conditions and limits stipulated by the legal and regulatory provisions, you have certain rights regarding the processing of your personal data, in particular:

– **Right to be informed about the use of your personal data (Article 13 of the GDPR):** The Bank has an obligation to provide you with clear information on the use of your data and on how to exercise your rights. As such, the Bank has established this Policy relating to the protection of personal data for information purposes.

– **Right of access to personal data processed by the Bank (Article 15 of the GDPR)**: you have the right to obtain confirmation of whether or not your personal data is processed, and if so, the right to access your personal data. The Bank will provide you with your personal data that is being processed within the limits of the applicable legal and regulatory provisions.

– **Right to rectification of personal data in the event of inaccurate or incomplete data (Article 16 of the GDPR)**: you may request that your data be amended in the event of inaccuracy or omission.

– **Right to erasure of personal data for legitimate reasons (Article 17 of the GDPR)**: you may request the deletion of your personal data from our databases, subject to certain exceptions, including use for evidential purposes in the event of litigation for the establishment, exercise or defence of legal rights by the Bank.

– **Right to request the restriction of the processing of personal data on legitimate grounds (Article 18 of the GDPR)**: you may request that the processing of your data be restricted. The right of restriction consists in asking for your personal data to be temporarily frozen, subject to meeting the conditions set out in Article 18 of the GDPR.

– **Right portability (Article 20 of the GDPR):** where your personal data has been collected with your consent or in the context of a contract and the processing of your data is carried out using automated processes, you may request the retrieval of the data you have provided to us, in a structured, commonly used and machine-readable format, for personal use or for transmission to a third party of your choice. In this context, you also have the right to have your personal data transferred directly from one controller to another where this is technically possible.

– **Right to object to the use of personal data for legitimate reasons (Article 21 of the GDPR):** you may object at any time, for reasons relating to your particular situation, to the processing of your personal data based in particular on the legitimate interests of the Bank when you consider that your interests, rights and freedoms take precedence over the processing or if the processing is based on reasons linked to business development.

If you refuse to provide certain personal data detailed in the Policy, or if you withdraw your consent, the Bank may be unable to carry out certain processing operations set out in the Policy.

The Bank ensures that the intellectual property rights and image rights of each data subject are preserved. In this context, in the event of an error on our Website, you can contact us.

You may submit a request to exercise the rights set forth above by sending a written request to the Data Protection Officer whose contact details are included in Section 2 of this Policy.

If you are not satisfied with the processing of your request, you have the right to lodge a complaint about the processing of your personal data by the Bank with a supervisory authority, in particular in the Member State in which you normally reside, your place of work or the place where the breach of your rights occurred.

In Luxembourg, the supervisory authority is the Commission nationale pour la protection des données, whose contact details are included below:

Commission nationale pour la protection des données
15, Boulevard du Jazz
L-4370 Belvaux, Luxembourg
Luxembourg

Telephone: (+352) 26 10 60 -1

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

14. Updating information 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.