

Policy on processing of Personal Data

The Bank, as “Data Controller” (namely the entity that determines the purposes and the means of processing of personal data), collects and processes the personal data (namely any information relating to an identified or identifiable natural person, the “Personal Data”) of each client. This Policy applies to all clients (i.e. natural persons and their proxyholders, as well as representatives/beneficial owners of legal entities) and prospects or potential clients showing an interest in a product or service offered by the Bank.

This Policy on processing of Personal Data (i) describes the Bank's obligations as Data Controller, (ii) indicates the rights of clients and prospects regarding the processing of their Personal Data, and (iii) provides them with the legally requisite information in this regard.

The Bank processes Personal Data in accordance with Regulation 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 (General Data Protection Regulation, hereinafter the “Regulation”).

The Bank undertakes not to sell the Personal Data of its customers and prospects as well as of any natural person for whom the Bank processes Personal Data.

1 Categories of Personal Data processed by the Bank

In the course of its business, the Bank collects and processes the following categories of Personal Data relating to clients and prospects, depending on the services for which they have subscribed or are about to subscribe:

- (i) personal identification data (e.g. name, address, phone numbers);
- (ii) personal details (e.g. gender, date of birth);
- (iii) official identification data (e.g. ID card number, Tax Identification Number (TIN));
- (iv) electronic identification data (e.g. email address, IP address, electronic signature);
- (v) biometric identifiers (e.g. dynamic signature);
- (vi) banking and financial data held by BIL or any other credit institution or payment service provider (e.g. bank account numbers and credit card numbers);
- (vii) financial transactions carried out through BIL or any other credit institution or payment service provider;
- (viii) data relating to the client's financial situation at BIL or any other credit institution or payment service provider (e.g. income, wealth, assets, loans, expenses);
- (ix) insurance related data (e.g. insurance company, type of insurance, amounts insured);
- (x) data relating to the person in question's business affairs (e.g. identity of legal representatives and other business contacts);
- (xi) data on habits and preferences (e.g. data collected during branch visits, when browsing our website www.bil.com and using our online forms, through connections to our online banking service BILnet, and from letters received from clients and prospects);
- (xii) recordings of electronic communications that do or could lead to transactions;
- (xiii) video recordings taken from CCTV systems inside and outside buildings and facilities, including ATMs;
- (xiv) telephone recordings.

With a view to meeting its legal obligations to combat money laundering and terrorism financing, as well as its duty of care regarding “know your client” requirements, plus whenever is strictly necessary, the Bank processes data about convictions and penalties, and about the holding of public mandates.

The Personal Data processed by the Bank may directly come (i) from the client or prospect or, where applicable, (ii) from public sources in order to fulfill its duty of care regarding “know your client” requirements.

2 Purposes of the processing of Personal Data

The client's Personal Data is or may be processed by the Bank, depending on the services for which the client has subscribed or is about to subscribe:

- (i) to the extent that such processing is necessary for the performance of the contracts between the Bank and the client or in order to take steps at the request of the client or prospect prior to entering into a contract. In particular, the Personal Data is processed for the implementation, administration and management of the contractual relationship and for the purpose of updating clients' or prospects' information;
- (ii) to the extent that such processing is necessary to comply with a legal obligation to which the Bank is subject, including in particular regulations relating to (i) precontractual information to be provided to clients or prospects on investment services involving financial instruments (MiFID), (ii) reporting obligations vis-à-vis the relevant Luxembourg and foreign authorities, (iii) good risk management by the Bank, (iv) measures to combat money laundering and financing of terrorism (v) “know your client” obligations, (vi) detection of fraudulent transactions, (vii) prevention of market abuse and (viii) prevention of any attempted fraud;
- (iii) to the extent that this processing is necessary in the Bank's legitimate interest in constantly upgrading its services in line with the needs of its clients, and in order to develop commercial strategies, but also for the Bank's business-related IT needs;
- (iv) insofar as this processing is necessary for the Bank's legitimate interest in overseeing the security of its staff, clients and prospects, in protecting the property for which it is responsible, and in preventing any kind of accident;
- (v) to the extent that this processing is based on the collection of consent for canvassing and marketing purposes relating to banking financial and insurance products, or other products promoted by the Bank.

3 Telephone recordings

The Bank is required to record telephone conversations that do or could lead to transactions, in order to meet several obligations:

- (i) retain proof of the transactions, check and/or confirm orders and instructions by telephone and/or clarify misunderstandings or correct errors when instructions are received and sent;
- (ii) show that the Bank has fulfilled its obligations to clients under the Markets in Financial Instruments Directive 2014/65/EU of 15 May 2014 (MiFID); and
- (iii) detect any behaviour involving insider trading or market manipulation in accordance with Regulation No 596/2014 of 16 April 2014 on market abuse.

4 Profiling activities and automated decision-making

For operational purposes and in order to provide its clients with the best possible service, the Bank uses profiling and automated decision-making.

The profiling mechanism involves a series of automated processing operations using Personal Data, with the following objectives:

- (i) to seek and identify the common characteristics of individuals likely to be interested in a specific new or existing bank product or service;
- (ii) to seek and identify a relatively homogeneous group of clients in terms of products acquired and/or banking behaviour in order to gain a better understanding of the Bank's business base and to personalise its commercial offerings.
- (iii) to collect and analyse information about clients' knowledge and financial experience, their attitude to risk and their financial situation in order to draw up a profile and offer suitable investment products, in accordance with our regulatory obligations as regards investor protection;
- (iv) to manage risk to which the Bank is exposed by analysing client banking behaviour (e.g. credit card use versus ability to repay), and to give clients better information about their financial situation and the risks inherent to specific requests (e.g. request to increase a credit card limit); and
- (v) to combat fraud, money laundering and terrorist financing by analysing client banking behaviour (e.g. transaction history) against a set of predefined criteria (e.g. target countries of transactions from the last six months) that enables the detection of suspicious activity.

The Bank has automated some decision-making in order to speed up the processing of requests and eliminate bias. This applies to requests to increase credit card limits and overdraft processing. Such decisions are thus based on an analysis of the client's banking behaviour, assets and borrowing.

Within the framework of automated decisions. The client has the right to request that the Bank re-examines his/her situation through the right to human intervention.

5 Third-party Personal Data

A client who provides the Bank with third-party Personal Data (e.g. of family members, relatives, agents, legal representatives, employees, company shareholders, managers, administrators or even beneficial owners) must obtain permission from said third-parties and inform them that the Bank processes Personal Data for the same purposes and in the same way as described in this Policy on the processing of Personal Data.

6 Collection and processing of Personal Data

The Bank collects only such information as is necessary for the provision of services to clients, and for compliance with its legal obligations.

Personal Data are collected from clients (e.g. when a client opens an account, by means of a questionnaire) and third parties (e.g. from duly instructed lawyers and notaries or national authorities, depending on the services provided).

Any refusal to disclose Personal Data to the Bank or refusal to allow the Bank to process such data, while being left to the discretion of the client, may impede the continuation of relations with the Bank, or preclude the provision of certain products or services by the Bank.

7 Persons with access to Personal Data and the objectives of such access

Personal Data may be transferred by the Bank to the following categories of recipient:

- (i) other financial institutions, including banks, insurers, tax specialists, payment and credit card issuers, interbank messaging platform managers, and online payment solution providers; all of these institutions acting as data controllers in relation to the services and products offered by the Bank (for example, processing a transaction involving a financial instrument, offering an insurance product, issuing a credit card, providing securities custody services, acting as the bank of the beneficiary of a payment, or producing a tax report);
- (ii) external service providers whose intervention is necessary for the services provided to clients, especially with regard to banking interfaces (e.g. transaction categorisation and account aggregation), information technology (e.g. operational IT task management, or management and hosting of technical infrastructure), physical security (e.g. cash transportation or CCTV management), printing (e.g. account statements), document and data management (e.g. secured destruction of documents, quality review, organization and retention of documents and data), consulting (e.g. on the development of new products and services), and communications (e.g. mailshot management); with all of these service providers acting as data processors on the Bank's behalf;
- (iii) external service providers whose involvement is necessary for the Bank to meet its legal and regulatory obligations, especially with regard to "know your client" requirements (e.g. through reports, in which case the service provider acts as data controller), identifying clients who are shareholders in certain companies and facilitating the exercise of their voting rights (e.g. by sending position reports to European issuers and information on general meetings sent to clients), reporting (e.g. formatting transactional reports to be sent to the financial regulator, in which case the service provider acts as data processor), and the audit or certification of the Bank's books (in which case the auditor acts as data controller).

These recipients of Personal Data must comply with their legal and contractual obligations regarding the protection of Personal Data, including applicable professional secrecy and confidentiality obligations.

The Bank may also transfer Personal Data if it has a legal or regulatory requirement to do so or is instructed to do so by a public authority, within the legal limits.

In accordance with legal and regulatory obligations concerning the mandatory exchange of tax information with participating countries, the Bank may have to disclose some of the Client's Personal Data to the Luxembourg tax authorities. The Luxembourg tax authorities may disclose the data communicated by the Bank to each competent foreign tax authority in accordance with applicable legal and regulatory requirements.

In some jurisdictions, the legal and regulatory provisions applicable to (transactions involving) financial instruments and similar rights require disclosure of the identity of the (in)direct holders or the beneficial owners of these instruments and their positions in said instruments. Non-compliance with these obligations may result in the financial instruments being blocked (where applicable, with the effect that voting rights may not be exercised, dividends and other rights may not be received, the financial instruments may not be sold or otherwise disposed of) or

in the imposition of any other penalties or restrictive measures provided for in the aforementioned provisions.

In the event of an investment in this type of financial instrument, clients must comply with applicable legal and regulatory provisions. To this end, the client expressly authorises the Bank to disclose, at its discretion, the identity of the client and/or of the beneficial owners as well as their positions in said financial instruments.

The Bank may also transfer personal data on the client's instructions.

As a rule, Personal Data is stored by the Bank and its service providers within the European Union. In the event of any transfer of Personal Data that would be necessary, the Bank will satisfy itself that an adequacy decision has been adopted by the European Commission or, where applicable, that suitable guarantees are in place (e.g. the adoption of standard data protection clauses, adherence to a code of conduct or certification).

8 Rights of natural persons

Natural persons have the right to access their Personal Data and to obtain a copy of it and, if such Personal Data are incomplete or incorrect, to have it rectified.

They also have the right to restrict the processing of their Personal Data, the right to object to its use and the right to have it erased by the Data Controller, under the conditions and within the limits specified in the Regulation and resulting in particular from the Bank's legal and contractual obligations. In all cases, natural persons may withdraw his/her for processing activities carried out for direct marketing purposes, without giving any reason. The management of their consent can be done at any time through BILnet.

They will also have the right to data portability, namely the right to receive their Personal Data or to require such data to be communicated to another Data Controller in a structured, commonly used and machine-readable format.

Natural persons may, at any time, withdraw consent that they have given in cases where the Bank has sought such consent for the processing of their Personal Data. The legality of the processing based on the consent granted before its withdrawal will not be affected.

In order to exercise the abovementioned rights, natural persons may submit a written, signed request proving their identity:

- via the BILnet secure messaging service, including: Data Protection / Request to exercise rights in the subject line
- by email to dpo@bil.com
- via the dedicated form available on our [BIL.com](https://survey.bil.com/?e=328967&d=l&h=7FB269DAC3609B7&l=en) website under the following link :
<https://survey.bil.com/?e=328967&d=l&h=7FB269DAC3609B7&l=en>

- by post to: Client Care Center, 69 route d'Esch, L-2953 Luxembourg.

However, in the event of a manifestly unfounded or excessive request, the Bank reserves the right to require payment of reasonable fees which consider the administrative costs incurred in providing the information, making the communications or taking the requested measures. Any request will be deemed excessive from the 3rd request made in the current year starting at the time of the first request. The Bank may therefore require the payment of fees equivalent to the research fees defined by its price list available on [BIL.com](https://www.bil.com).

If the response received has not been entirely satisfactory to him or for any question relating to data protection, the natural person has the possibility to refer to the Data Protection Officer by contacting him either via the BILnet secure messaging service, or by email at the following address: dpo@bil.com, or by mail to the following address Data Protection Officer, 69 route d'Esch L-2953 Luxembourg.

They may also file a complaint with Luxembourg's National Commission for Data Protection (CNPD) by sending a letter to 15, boulevard du Jazz, L-4370 Belvaux, or by completing the online form which is available on the CNPD's website under Individuals -> Asserting your rights.

9 Period of retention of Personal Data

Personal Data will be stored by the Bank for no longer than is necessary for the purposes for which the Personal Data are processed by the Bank and in accordance with its legal obligations, i.e. 10 years after the end of the business relationship with clients. Prospects' Personal Data is stored for a period of two years from its collection.

Exceptionally (legal interruption and suspension of storage periods), the Bank may store data beyond the periods mentioned above, in accordance with applicable legal provisions.

10 Personal Data security

The Bank protects Personal Data and keeps it confidential. To that end, the Bank implements technical and organisational measures that include:

- Informing and training the Bank's staff about their data protection obligations;
- Factoring data protection implications into the design of products, services and features offered by the Bank;
- Establishing an information security framework;
- Contractually requiring the Bank's data processors to demonstrate and implement a similar level of data protection, in accordance with the General Data Protection Regulation.