



# DATA PROTECTION POLICY



## 1. PURPOSE

BIL (the Bank hereafter) is a key player in the Luxembourgish financial market and has also dedicated wealth management offices in Switzerland and China as well as trading floors in Luxembourg and Zurich. We offer a broad range of services – from retail banking to insurance going through private banking, corporate banking and financial markets – to meet the needs of our local and international clients.

As of May 25 2018, the protection of personal data is reinforced in the European Union by the General Data Protection Regulation (the "General Data Protection Regulation Data Protection Regulation" or the "GDPR" hereafter). This increases the responsibility of businesses and also enshrines new rights for individuals. In the course of our activities and services, we process personal data. Our goal is conduct such processing in accordance with applicable data protection laws and regulations, including GDPR. This Data Protection Policy ("Policy" hereafter) discloses our commitments to ensure privacy protection and responsible collect and use of personal data. It is fully integrated into the Bank's Terms and Conditions.

Through this policy, BIL applies the principles laid down by the United Nations Global Compact, and more specifically Principle 10 on anti-corruption : Businesses should work against corruption in all its forms, including extortion and bribery.

Additionally, this policy is aligned with the 2030 Agenda and the Sustainable Development Goals (SDG) and specifically with SDG 16: Peace, justice and strong institutions.

## 2. SCOPE

This Policy is relevant to all BIL employees worldwide, business partners (service providers, clients, etc.) and all natural persons in contact with BIL Group. This Policy applies transversally to all personal data processed within the framework of the activities carried out by BIL Group. In those situations where the Bank does not have full management control, we will exercise our available leverage to influence compliance with this Policy. BIL will always comply with applicable local laws that are in force. In situations where there is a conflict with international norms, we shall seek to uphold our company values - defined in our Code of Ethics – and develop a response on a case-by-case basis.

## 3. DEFINITIONS

The Bank is committed to take appropriate technical and organizational designed (i) to enable the effective application of data protection principles and (ii) to incorporate the necessary safeguards into the processing, thereby enabling the Bank to meet its legal obligations and to protect the rights of data subjects.

- **Data subject:** An identifiable natural person whose personal data is processed by BIL.
- **Personal data:** Any information relating to an identified or identifiable natural person ("data subject") an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity. This is data that is both provided to us directly and generated by using our services.

- **Processing:** Any operation or set of operations carried out or not carried out by means of automated processes and applied to personal data, such as the collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, reconciliation or restriction, deletion or destruction.
- **Data controller:** 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 of personal data; where the purposes and means of such processing are determined by EU or Member State law, the controller or may be designated or specific criteria for designation may be provided by the law of the Union or by the law of a Member State. BIL is responsible for the processing and is represented by its Management Board in charge of the processing of personal data.
- **Data processor:** A natural or legal person, public authority, department or other body that processes body that processes personal data on behalf of BIL.
- **Consent of the data subject:** Any manifestation of free will, specific, informed and unambiguous expression of will by which the data subject accepts, by a declaration or by a clear positive act, that personal data concerning him/her are processed.

#### 4. COMMITMENTS

BIL Group's Management Boards and employees process personal data with all due care so that only necessary and accurate personal data are processed by authorized employees, in a legitimate, secure and transparent manner, and for specific and limited purposes. To this end, the Bank is committed to the following principles regarding the processing of personal data:

##### 4.1. Lawfulness

BIL Group is committed to process personal data in a legitimate manner. We process personal data if (at least) one of the following lawful processing grounds applies :

- where the processing is based on consent;
- if the processing is necessary for the performance of a contract;
- if the processing is necessary for compliance with a legal obligation legal obligation;
- if the processing is necessary to safeguard a vital interest;
- if the processing is necessary for the performance of a task in the public interest or for the exercise of official authority; and/or
- if the processing is necessary for the purposes of the legitimate interests pursued by BIL Group or by a third party.

##### 4.2. Honesty and transparency

The processing of personal data is carried out with the utmost transparency towards the data subjects to enable them to understand why and how their personal data is used by BIL Group, as well as their rights in terms of data protection. This transparency is a prerequisite for fair processing as it allows data subjects to maintain control over their personal data.

### **4.3. Purpose limitation**

The Bank is committed to collect personal data for specific, explicit and legitimate purposes. Any re-use of personal data for purposes other than those originally intended is not allowed, unless the data subjects have given their consent, have been informed or where such re-use is authorized by a law of the European Union or one of its Member States.

### **4.4. Data minimization and accuracy**

The Bank is committed to ensure that personal data processed is adequate, relevant and limited to what is necessary.

In accordance with the relevant internal policies and procedures, all reasonable steps to maintain the accuracy of personal data shall be taken.

In view of the purposes for which they are processed, personal data that is incorrect will be rectified or deleted without delay.

### **4.5. Limitation of retention**

The Bank is committed to not retain personal data (including data on documents) for longer than necessary. BIL Group's Management Boards and employees ensure that a data retention period is specified for each processing activity for which they are responsible, in accordance with applicable internal policies and procedures and/or legal obligations.

At the end of the retention periods, personal data will be destroyed, deleted or anonymized in accordance with applicable internal policies and procedures.

### **4.6. Integrity, security and confidentiality**

The Bank is committed to process personal data in such a way as to ensure appropriate security. In particular, the Bank takes care to prevent unauthorized or unlawful processing and loss, destruction or damage of accidental origin.

In this respect, BIL Group's Management Boards and employees update their knowledge of internal policies and procedures relating to information security.

BIL Group's Management Board and employees are required to report personal data breaches in a timely manner in accordance with the relevant internal policies and procedures.

## **5. RIGHTS OF DATA SUBJECTS**

Pursuing the GDPR, data subjects have various rights with respect to their personal data, including :

- **Right of information** : At the time of collection of personal data and in accordance with applicable data protection laws and regulations, BIL provides data subjects with appropriate information on how their personal data is processed and their rights as data subjects.

- **Right of access** : right to obtain a confirmation of the actual processing of his or her personal data and, if so, to access the personal data.
- **Right of rectification** : right to have inaccurate personal data relating to him/her corrected.
- **Right of erasure** : (the right to be forgotten) : right to have his or her personal data erased. This right must be considered by BIL in light of other applicable laws and regulations that would require the retention of information for a for a specific period of time.
- **Right of restrictions of processing** : right to request the Bank to restrict the processing of personal data.
- **Right of data portability** : right to receive the personal data that he or she has provided to BIL in a structured and machine-readable format and to transmit such personal data to another organization.
- **Right to objection to processing** : right to object at any time to the processing of personal data concerning him or her based on the legitimate interest pursued by BIL.
- **Right to withdraw consent** : if the data subject has consented to the processing of his/her personal data, he/she has the right to withdraw such consent.

## 6. RECIPIENTS OF PERSONAL DATA

In order to carry out the processing activities in accordance with the legal bases set out by each Data controller, BIL may send some personal data to internal and external recipients:

- Organizational parts of BIL (i.e. any department of BIL that may help achieve the purpose pursued by the Data controller);
- Entities of BIL Group;
- Public authorities (e.g. public prosecutor, collector general of taxes, national social security, etc.);
- External organizations (e.g. Data processor, brokers and insurers, notaries, lawyers, etc);
- Internal and/or external auditors.

## 7. CATEGORIES OF DATA PROCESSED

The processing activities carried out by BIL imply the processing of the following categories of personal data:

- Identification information (e.g. the data subject's first and last name, date of birth, place of birth);
- Professional information (e.g. position, employer);
- Contact details (e.g. email address, postal address, phone number);
- Economic and financial data (e.g. transactions, account number, income);
- National identification number (e.g. social security number);
- Official documents (e.g. identity card, driver's licence).

The processing of specific categories of personal data is prohibited. The following are considered as specific categories of personal data :

- data revealing racial or ethnic origin;
- political opinions, religious or philosophical beliefs or trade union membership;
- genetic data, biometric data for the purpose of uniquely identifying an individual a natural person in a unique way;
- data concerning the health, sex life or sexual orientation of a natural person.

Processing for marketing purposes, including newsletters and surveys, is strictly controlled and centralized as much as possible at the level of BIL Luxembourg or entities. The legitimate interest as a legal basis may be invoked to justify the processing only for existing clients and for the sole purpose of promoting similar products and services. Any other marketing campaign will be based on the consent of the data subjects.

When determining and carrying out profiling activities, the Bank pays particular attention to the transparency, honesty and security of the processing and bears in mind that this type of processing is significant because of its sensitive nature.

In addition, whenever an automated individual decision is made, it is ensured that (at least) one of the following conditions is met:

- such a decision is necessary for the conclusion or performance of a contract between the data subject and BIL Group;
- such a decision is authorized by the applicable legal and regulatory provisions applicable laws and regulations;
- such a decision is based on the explicit consent of the data subject.

## **8. INTERNATIONAL DATA TRANSFER**

Whenever transfers of personal data to third countries are planned, such international data transfers will take place if :

- An adequacy decision from the European Commission applies, meaning that the country of destination offers an adequate level of data protection ;
- Appropriate safeguards have been put in place, such as binding corporate rules or a data transfer agreement on the basis of EU standard contractual clauses.

## **9. COOKIES**

Please refer to our "Data Protection at BIL" section on BIL's website for more information about our use of cookies (<https://www.bil.com/en/bil-group/documentation/Pages/data-protection.aspx>).

## **10. IMPLEMENTATION**

The Bank is committed to:

- Embed the Data Protection Policy throughout the Group through internal communication.
- Raise awareness among new joiners together with the other Compliance topics.
- Provide all employees with comprehensive compliance training on data protection to ensure the lawfulness of the processing of personal data.
- Implement disciplinary and criminal sanctions in case of failure to comply with this Policy.

## **11. GOVERNANCE**

The Chief Compliance Officer of BIL is responsible for this Policy, but the local Compliance Officers of the branches and subsidiaries are responsible for establishing effective local systems, controls and procedures relating to the matters covered by this Policy. The IT Security Officer, the Head of Physical

Security and the Chief Information Security Officer guarantee the security of the processing of personal data for which the BIL Group is responsible. The Data Protection Officer (DPO), supported by the Data Protection Contacts, is responsible for advise the Bank and its employees, monitor compliance with applicable data protection laws and regulations, and facilitate cooperation between the Bank and the Data Protection Authority by acting as a contact point. In addition, the members of the BIL hierarchy whose teams process personal data are responsible for their employees' compliance with the applicable legal obligations contained in the GDPR. The Internal Control Committee (ICC) is the body to which the Data Protection Officer reports on compliance with the legal obligations regarding data protection within BIL. In any case, all employees are bound by professional secrecy. Additionally, in case of an exceptional situation that because of its relevance should be reported at higher level, it will be reported directly to the Board of Directors.

## **12. COMPLIANCE & MONITORING**

Our Data Protection Policy will be updated regularly in order to take into consideration legal and regulatory requirements changes.

## **13. REPORTING**

The Bank will monitor and report, whenever it is possible, on a regular basis relevant KPIs related to the issues covered along this policy. For more information on the steps we take to ensure that our operations uphold our commitments to personal data protection, and how we measure progress to those commitments, please consult our CSR reports available on our website at: <https://www.bil.com/sustainability/reports.html>

## **14. REVIEW**

The Bank will periodically review this Policy to evaluate continued relevance, monitor compliance and drive continual improvement. We also welcome feedback from, and dialogue with, interested parties. All feedback and comments on this Policy should be sent to [sustainability@bil.com](mailto:sustainability@bil.com)

**Marie Bourlond, Chief Compliance Officer**

**16/12/2021**