CIBC Colombian Entities Privacy Policy

In accordance with law 1581 of 2012 and Decree 1074 of 2015, this Privacy Policy ("Policy") discloses the privacy practices for the Canadian Imperial Bank of Commerce and its wholly-owned subsidiaries (collectively "CIBC") in connection with its operations in Colombia. This Policy applies to the collection and processing of any personal data collected by CIBC in the course of conducting its business in Colombia and describes the purposes set forth by CIBC for such collection and processing.

1. Terms

In this Policy;

- "clients" means clients of CIBC whose personal data is collected or processed in Colombia;
- "individuals" means any individuals that can be identified, directly or indirectly, by personal data that has been collected or processed in Colombia by CIBC; and
- "personal data" means any information relating to an identified or identifiable individual (natural person).

2. Data Controllers

Among CIBC entities, two of them will act as Data Controllers in Colombia:

I. CIBC Financial Advisory Latin America S.A.S. ("FALA")

Location: Bogotá D.C., Colombia.

Address: Carrera 7 No. 71-21 Torre B Oficina 504, Postal Code 110221

Email: CIBCColombiaPrivacy@cibc.com

Telephone number: +571 516 9047

II. Canadian Imperial Bank of Commerce

Location: Toronto, Ontario, Canada.

Address: Commerce Court, Postal Code M5L 1A2

Email: client.care@cibc.com

Telephone number: 1-800-465-2422

3. Data Processing Purposes

CIBC clients' personal data is collected, recorded, organized, stored, used, and deleted for the following purposes, to:

- establish clients' identity and determine their eligibility for products or services;
- help to ensure that the advice, products or services offered to or purchased by the clients are appropriate for them;

- set up, manage, administer and maintain the products or services of the clients;
- send communications to the clients by various methods, such as mail, e-mail, text (SMS), telephone, automatic dialing-announcing device (at the numbers you have provided to us), fax, or other telecommunication channels, or social media, including marketing or communications about benefits, features or other details about products or services offered by CIBC;
- review and analyze clients' applications, transactions and other information to understand who the clients are, their financial needs and activities, and what products, services, and promotions may be of his interest, including targeting promotions based on information that the Data Controllers have collected;
- better manage and improve clients' relationship with CIBC including monitoring, reviewing or improving client service and business processes to make it easier to do business with CIBC;
- encourage the clients to continue doing business with CIBC;
- perform CIBC everyday business and operations including record keeping or internal reporting;
- understand and better manage CIBC's business and to develop products and services, including conducting market research or analyzing data CIBC holds about the clients;
- administer referral arrangements;
- use third-party service providers to perform services on behalf of CIBC;
- manage CIBC's credit, business and other risks as may be required to operate as an effective, efficient and financially prudent financial institution;
- meet tax, legal and any other regulatory obligations;
- protect the clients and CIBC from error and criminal activity including the prevention, detection and investigation of fraud, money laundering, cyber threats and other such risks and threats (e.g., we will review and analyze your applications, transactions and other information to help us identify various types of threats and risks such as credit, fraud, and money laundering);
- share personal data within CIBC or with third parties including:
  - accounts holders or representatives in connection with the product or service or service separately or jointly obtained;
  - appropriate legal or governmental authorities to protect the client of a fraud, financial abuse, or other illegal activity or where CIBC has reasonable grounds to believe that my interests can best be served by taking action;
  - appropriate legal or governmental authorities to protect CIBC rights or interests (e.g. where CIBC is involved in judicial, administrative or regulatory proceedings, or other similar processes), or, in order to comply with any legal and regulatory obligations.

FALA may collect and process clients' personal data in Colombia on behalf of CIBC and for all the purposes described above. Therefore, FALA should be considered as a Data Processor for purposes of such personal data.

4. Personal data international transfers

Personal data may be stored and processed in any country where the Data Controllers have affiliates or service providers. Therefore, the personal data can be transferred to countries outside of Colombia, including Canada, the United States, the United Kingdom, Hong Kong, Singapore, China, Japan and Australia which may provide for different data protection rules.

5. Data protection rights

In accordance with Colombian data protection regulation, individuals have the following rights, to:

- Access, update and rectify their personal data. These rights can be exercised when the Data Controllers have collected inaccurate or incomplete personal data. Jointly, these rights proceed when data processing violates Colombian data protection regulation.
- Require a copy of the consent provided to the Data Controller, unless there is a legal obligation to collect and process this personal data.
- Know the purposes of the personal data processing.
- Exercise individuals' suppression and deletion rights. This is also possible when Data Controllers have not complied with Colombian data protection regulation requirements.
- Have free access to their personal data stored by the Data Controllers.
- Submit a complaint to the Colombian Superintendence of Industry and Commerce, if the procedure for answering complaints and queries set forth by Data Controllers has not provided an answer or the answer is not satisfactory.

6. Person in charge of internal data protection procedures

- CIBC's Executive Director is the person in charge of answering complaints and following legally established proceedings.
- FALA's Managing Director is the person in charge of answering complaints and following legally established proceedings.

7. Procedure and deadlines for answering complaints and queries from individuals

Procedures and deadlines for answering personal data requests and complaints related to data protection are described in Section 7.1 and Section 7.2 below.

7.1 Procedure and deadlines for answering personal data requests

Individuals or their legal representatives, may access their personal data processed and stored by the Data Controllers. Personal data requests must be sent to the following email addresses:

- CIBC: CIBCColombiaPrivacy@cibc.com
- FALA: CIBCColombiaPrivacy@cibc.com

An individual's identity is previously verified in order to avoid unauthorized access to the personal data processed by the Data Controllers. When the request is sent by a person that does not sufficiently demonstrate their legal representation of the individual, Data Controllers will discard such request.

The information request must be answered within ten (10) business days after the date in which the request is received. If for any reason the request cannot be answered in the legal term described above, Data Controllers will inform of this situation to the individuals or their representatives. Additionally, Data Controllers will inform the reasons for the delay and will inform a new deadline to answer the request. The new deadline should be of maximum five (5) additional days to the ten first days initially granted.

7.2 Procedure and deadlines for answering complaints related to data protection

Individuals or their legal representatives can submit a complaint, if they consider that the personal data collected and processed by the Data Controllers must be corrected, updated, rectified, or that Data Controllers do not comply with Colombian regulation.

These complaints must be sent to the following email addresses:

- CIBC: CIBCColombiaPrivacy@cibc.com
- FALA: CIBCColombiaPrivacy@cibc.com

The procedure to process and answer data protection complaints has the following steps:

a) Individual's identity is previously verified in order to avoid unauthorized access to the personal data processed by the Data Controllers. When the request is sent by a person that does not sufficiently demonstrate that is the legal representative of the individual, Data Controllers will discard the complaint.

b) Data Controllers verify that the following information is included in the complaint submitted:

   (i) Individual's identification information (name and id number)

   (ii) Personal contact information of the individual that makes the complaint (home address, personal email and telephone number).

   (iii) Copy of the individual's ID or documents that demonstrate that they have legal faculties to represent the individual.

   (iv) A clear and precise description of the personal data that motivated the complaint.

   (v) A description of the facts that justify the complaint.

   (vi) Any additional documents that the person considers necessary to sustain the complaint.

   (vii) Individual's signature.

   (viii) The original copy of the complaint.

c) If the complaint provides incomplete information, Data Controllers will inform the individuals within the next five (5) business days, following the day the complaint is received, in order to complete it. If the individual does not complete the complaint within the next two (2) months after the information request is sent by the Data Controllers, the complaint will be discarded.

d) If the complaint is received by a person or area other than the area or person described in section 5 of this Policy, they will inform the person in charge within the next two (2) business days. Additionally, the person that initially receives the complaint will inform of this situation to the complainant.

e) Once the complaint with all the required information is received, the Data Controllers will mark the personal data with the following phrase "complaint currently under review", and the reasons for such complaint. This legend must be placed within two (2) business day. Additionally, this legend will remain until the complaint is finally answered by the Data Controllers.

f) The complaint must be answered within fifteen (15) business days after the date in which the request is received. If for any reason the complaint cannot be answered within the legal term described above, Data Controllers will inform of this situation to the individual. Additionally, Data Controllers will inform the reasons for the delay and will define a new deadline to answer the request. The new deadline should be of maximum eight (8) additional days to the fifteen (15) days initially granted.

8. Data Suppression rights

Individuals can request the suppression of their personal data in any of the following circumstances:

- When an individual considers that the data processing made by a Data Controller does not comply with Colombian data protection regulation.
- The personal data stored by the Data Controllers is not necessary for the data processing purposes previously authorized.
- The period of time to fulfill data processing purposes has already expired.

However, the suppression right can be restricted in the following cases:

- The suppression request will not proceed if there is a legal or contract obligation that requires Data Controllers to keep the personal data.
- The suppression of personal data can obstruct an administrative investigation or judicial proceedings related to tax obligations, criminal acts or administrative sanctions.
- Personal data is required for the defense of legally protected interests, to initiate and action in public interest or to comply with legal obligations.

9. Withdrawal of privacy consent

Individuals can withdraw their consent at any moment, unless there is a legal or contract obligation that requires the data processing to continue.

10. Information Security

CIBC and FALA take the protection of personal data seriously. Data Controllers make reasonable efforts to prevent unauthorized use, sharing, loss or theft of information.

Data Controller's employees who have access to personal data are made aware of the importance of keeping it confidential. Depending on the nature of the information, it may be stored in the office that individuals deal with, in various computer systems, or in the record storage facilities of CIBC or service providers.

Data Controllers use service providers who might have access to personal data. These providers are carefully selected and Data Controllers require them to have privacy and security standards that meet Data Controllers' requirements. Data Controllers use contracts and other measures with our service providers to maintain the confidentiality and security of the personal data and to prevent it from being used for any other purpose.

Data Controllers, service providers and other parties, including CIBC affiliates, with whom personal data is shared under this Policy, may perform activities outside of Colombia. As a result, personal data may be securely used, stored or accessed in other countries and be subject to the laws of those countries. For example, information may be shared in response to valid demands or requests from government authorities, courts and law enforcement officials in those countries.

11. Policy's date of entry into force and personal data conservation periods

This Policy entered into force November, 2017.

The length of time CIBC keeps clients' personal data will vary depending on the product or service and the type of the information. CIBC keeps the information for as long as it is reasonably needed for customer service, legal or reasonable business purposes. For these reasons, CIBC keeps personal information beyond the end of the relationship with its clients. When the information is no longer required, it is securely destroyed.