



Summary Personal Information Protection Policy

This document is a summary (the “**Summary**”) of Laurentian Bank of Canada Financial Group’s (“**LBCFG**”) Personal Information Protection Policy (the “**Policy**”). Since the Policy is reviewed and amended from time to time, this Summary may not fully reflect the up-to-date version of the Policy. In the event of a conflict between the content of this Summary and the provisions of the Policy, the Policy shall prevail.

1. PURPOSE AND SCOPE

LBCFG is subject to various statutory, regulatory and contractual obligations in connection with privacy in the jurisdictions in which it operates. The Policy is part of the risk appetite and management framework of LBCFG. Specifically, it outlines the framework used to identify, manage, measure, mitigate, and report significant privacy risk. Thus, the main objectives of the Policy include the following:

- Promoting a standardized privacy compliance culture across LBCFG;
- Raising awareness regarding the risks inherent to the handling of personal information;
- Stipulating the allocation of responsibilities;
- Adopting good working practices with respect to privacy;
- Implementing measures to ensure that regulatory obligations are met;
- Responding to requests to access personal information diligently and efficiently; and
- Establishing a standardized process for dealing with privacy breaches.

The Policy applies to all lines of business and sectors of LBCFG and includes their related support functions, whether performed by LBCFG or on behalf of LBCFG. It applies to all personal information collected and processed by LBCFG, regardless of the jurisdiction where it is held.

2. CONTENT

The Policy sets out some of the obligations of LBCFG in connection with the proper and secure collection, use, disclosure, retention and destruction of personal information. It is built upon ten (10) privacy principles set out in the federal *Personal Information Protection and Electronic Documents Act*, namely:

- **Accountability and management.** LBCFG is responsible for the personal information under its control. LBCFG’s privacy framework relies on three (3) levels of responsibility (or “lines of defence”) that can be described as follows: (i) each line of business and sector of LBCFG, including its designated Assistant Privacy Officer (“**APO**”), has primary responsibility for managing privacy; (ii) a Chief Privacy Officer (“**CPO**”) leads the second line of defence together with other oversight functions, and provides independent verification of the effectiveness of the first line of defence; and (iii) internal audit acts as a third line of defence and provides assurance on the effectiveness of the privacy. The relevant roles, responsibilities and duties of each line of defence as well as of the employees, board of directors and board committees of LBCFG, generally, are detailed in the Policy;
- **Identifying purposes for the collection of personal information.** At or prior to the collection of personal information, each line of business and sector shall define and document the identified purposes for which they need to collect personal information, identify the personal information that is being collected, properly notify and explain, as needed, to the concerned individuals the identified purposes, and ensure that personal information is collected only for the identified purposes;
- **Consent.** Each line of business and sector must obtain the consent, whether express or implied, of the individual whose personal information is collected, used or disclosed. As new uses for information become available, it may also be necessary to obtain renewed consent. The Policy distinguishes how express or

implied consent is obtained in a number of common situations. It also details how a client may withdraw or refuse to give his or her consent and the procedures that apply in these situations;

- **Limiting collection.** Each line of business and sector is required to limit the amount and type of information collected to what is necessary for the identified purposes. Therefore, each line of business and sector must identify in its information-handling process and procedures the kind of personal information that is collected, and why it is needed;
- **Limiting use, disclosure and retention.** Each line of business and sector shall not use or disclose personal information for purposes other than the identified purposes for which it was collected, except with the consent of the individual or as required or permitted by law. The Policy provides a non-exhaustive list of exceptional circumstances in which personal information can or must be disclosed without the concerned individual's consent. Regarding the retention of personal information, the Policy provides that each line of business and sector shall maintain proper records detailing any disclosure of personal information to third parties, subject to exceptions where personal information is made available to third parties in connection with ongoing activities. Each line of business and sector has retention schedules aligned with applicable laws and appropriate business considerations, as well as standards and procedures specifying how to properly dispose of personal information;
- **Accuracy.** Each line of business and sector shall make reasonable efforts to ensure that personal information used on an ongoing basis is complete, accurate and up-to-date, unless limits to the requirement for accuracy have been clearly set out by the applicable laws, regulations or adopted industry standards. The Policy sets out that a client may challenge the accuracy and completeness of his or her personal information and have it amended as appropriate;
- **Safeguards.** Each line of business and sector must protect the security of personal Information in their custody or under their control, regardless of the format in which it is held. Reasonable and appropriate physical, administrative, and technical safeguards to protect personal information against loss, theft, cyber incidents and unauthorized access, disclosure, use or modification must be used. The Policy specifically refers to the principles and procedures contained in LBCFG's Information Technology Risk Management Policies and Standards;
- **Openness.** All client-facing material on LBCFG's policies and practices relating to the management of personal information shall be readily accessible and easily understandable;
- **Individual access.** Subject to a number of exceptions, clients are entitled to know, upon request, which personal information each line of business and sector is holding about them. Clients are entitled to access their personal information and to know to which third parties said information has been disclosed. The Policy sets timing requirements for the fulfilment of personal information access requests. It also provides a non-exhaustive list of circumstances in which access to personal information may be denied; and
- **Monitoring and enforcement.** Clients have the right to submit privacy inquiries and privacy complaints relating to the handling of their personal information or compliance with privacy obligations. It follows that each line of business and sector must ensure that there is an adequate complaint and dispute resolution process in place, and that the process is effective, fair, confidential, easy-to-use, timely and properly recorded. Clients must be informed of the existence of such mechanisms and all complaints shall be investigated, in accordance with the Policy.

3. ENFORCEMENT

Compliance with the Policy is mandatory and binding for LBCFG's employees. Any employee who violates the Policy or its related procedures or instructions is subject to immediate disciplinary measures, which may include dismissal or civil or criminal proceedings.

4. REVIEW

The Policy is reviewed at least annually by the CPO and is submitted to the Executive Committee (or the Corporate Risk Committee as delegated by the Executive Committee) of LBCFG for approval and subsequently approved by the Risk Management Committee of the board of directors of LBCFG.

October 2021