Otéra
CDPQ

# Policy respecting the Protection of Personal Information

Legal Affairs and Corporate Secretariat
March 31, 2023

# Policy respecting the Protection of Personal Information

| Team | Objective |
|---|---|
| Legal Affairs and Corporate Secretariat | To oversee the management of personal information in accordance with applicable laws and regulations. This policy is addressed to all Otera employees. |

| Action | Approval authority | Date |
|---|---|---|
| Entry into force | Executive Committee | 2014-03-13 |
| Amendment | Executive Committee | 2017-05-18 |
| Administrative amendment | Vice-President, Human Resources and Corporate Services | 2017-10-18 |
| Administrative amendment | Vice-President, Human Resources and Corporate Services | 2018-05-31 |
| Administrative amendment | Vice-President, Human Resources and Corporate Services | 2019-11-27 |
| Consolidation | Board of Directors | 2022-11-29 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Table of Contents

Otéra is committed to maintaining the confidentiality, security and accuracy of Personal Information. This policy describes the principles that Otéra must respect in the collection, use, retention and communication of Personal Information as well as any Processing of Personal Information.

# 1. Definitions

In this policy, terms that are not defined in the main text are defined in Appendix 1.

# 2. Scope

Otéra and its Employees shall comply with the Laws respecting the protection of personal information in the context of any Processing of Personal Information, particularly of its Employees, customers, partners and suppliers.

This Policy applies to Personal Information relating to identifiable individuals (collectively, “Data Subjects”) collected by Otéra or disclosed to Otéra by third parties, such as service providers and business partners, including, without limitation, Personal Information:

- of Employees;
- of members of the general public who contact Otéra for information, including about its service offer;
- of potential borrowers, partners, suppliers or customers when Personal Information is collected in the course of their professional interactions with Otéra and its Employees;
- of candidates for a position offered by Otéra;
- of visitors to Otéra’s offices and website.

By delegation from the President and Chief Executive Officer, Otéra has designated a person responsible for the protection of Personal Information (the “Privacy Officer”), whose title, contact information and date of appointment are communicated to the *Commission d’accès à l’information*.

The role of the Privacy Officer is described in Section 7 of the Guidelines.

# 3. Application

This policy applies to all Employees who have access to Personal Information in the course of their duties. The protection of Personal Information is the responsibility of each Employee. All Employees who process Personal Information shall review, understand and comply with this Policy. In addition, they shall act in accordance with the requirements set out in this Policy.

# 4. Principles

Otéra adopts Guidelines that detail the responsibilities and obligations with respect to the protection of Personal Information, according to the following principles:

- **Collection**: In the course of its activities, Otéra collects Personal Information limited to that which is strictly necessary for the purposes for which it is collected.

- **Use**: Personal Information can only be used for the legal or legitimate business purposes identified by Otéra at or before the time of collection.

- **Communication**: Personal Information processed within Otéra is accessible or communicated only to Otéra Employees who need it to perform their duties. Otéra may disclose to third parties the Personal Information they need to assist Otéra in fulfilling the purposes it has identified before or at the time of collection by working with those third parties to protect the Personal Information it has disclosed for those purposes.

- **Legal basis**: Where required, Otéra obtains prior valid consent from the Data Subjects before processing their Personal Information for the specific legitimate business purposes identified by Otéra before or at the time of collection. To the extent applicable, the GDPR allows Otéra to rely on other legal basis in addition to consent for the Processing of Personal Information, depending on the purpose for which Otéra processes Personal Information.

- **Retention**: Otéra strives to retain Personal Information only as long as necessary to fulfill the purposes for which it was collected.

- **Security and Privacy Incidents**: Data security is of the outmost importance to Otéra. Otéra strives to maintain physical, technical and administrative safeguards that are adequate given the sensitivity of the Personal Information it aims to protect. Employees shall remain vigilant regarding Privacy Incidents and shall immediately report any actual or reasonably suspected Incident to the Incident Management Committee. This will allow Otéra to promptly investigate the Incident, to respond to it in accordance with its Information Security Incident Response Plan and in accordance with policies and Guidelines, and to protect Otéra, the Data Subjects and any other organizations from damages that may result therefrom.

# 5. Complaints

- **Employees**. Employees who have reason to believe that there has been a violation of Applicable Laws or this Policy, or who wish to submit a complaint regarding Otéra's processing of Personal Information, are encouraged to report their concerns directly to their supervisor, who may consult with the Privacy Officer, if necessary. In addition, Employees who receive a complaint related to the Processing of Personal Information from a Data Subject must promptly report the complaint and the name and contact information of the complainant (if available) to the Privacy Officer.

- **Data Subject other than an Employee**. Any Data Subject other than an Employee who has reason to believe that there has been a violation of Applicable Laws or of this policy, or who wishes to complain about Otéra's Personal Information Processing practices, is invited to submit a written complaint to renseignementpersonnel@oteracapital.com.

# 6. Contact

For any request regarding Personal Information and for any questions or comments, please contact the Privacy Officer:

Chief, Ethics and Compliance
Otéra Capital
Édifice Jacques-Parizeau
1001, Square-Victoria Street, Suite C-200
Montréal (Québec) H2Z 2B5
Canada
renseignementpersonnel@oteracapital.com

# 7. Governance

The Board of Directors, upon the recommendation of the Governance and Ethics Committee, shall approve this policy.

The Executive Committee shall recommend this policy to the Governance and Ethics Committee.

The Legal Affairs and Corporate Secretariat Group shall establish and maintain the policy management framework and report annually to the Executive Committee and the Governance and Ethics Committee on its application. The Legal Affairs and Corporate Secretariat Group shall promptly notify the Executive Committee and the Governance and Ethics Committee of any material Confidentiality Incident.

# 8. Review

This policy shall be reviewed at least every three years.

# Appendix 1: Definitions

For the purposes of this policy:

**“Board of Directors”** means the Board of Directors of Holding Otéra Capital Inc.

**“CDPQ”** means the *Caisse de dépôt et placement du Québec*.

**“Confidentiality Incident Register”** means a file documenting all Confidentiality Incidents suffered by Otéra, whether or not such Incidents have been notified to the competent supervisory authority and to the Data Subjects.

**“Employees”** means all employees, consultants, officers, or directors of Otéra.

**“Executive Committee”** means the Executive Committee of Otéra Capital Inc.

**“Governance and Ethics Committee”** means the Governance and Ethics Committee of Holding Otéra Capital Inc.

**“Guidelines”** means the guidelines on the protection of Personal Information.

**“Incident Management Committee”** means the committee appointed under the Information Security Incident Response Plan.

**“Incident”** or **“Confidentiality Incident”** means unauthorized access to Personal Information, unauthorized use of Personal Information, unauthorized communication of Personal Information, or loss of Personal Information or any other breach of the protection of such information. Such as in the following cases:

- Accident: Personal Information is disclosed to the wrong person by accident. For example (i) an email containing Personal Information is sent to the wrong address due to a mechanical or human error; (ii) Personal Information is made public on Otéra’s website following a technical problem.
- Loss: Personal Information is lost. For example an Employee’s laptop, mobile device or briefcase containing Personal Information is lost.
- Unauthorized access, use or communication: Personal Information is accessed, used or communicated by an unauthorized person, or in an unauthorized manner, or for an unauthorized purpose, including in violation of one of Otéra’s policies or the Applicable Law. For example (i) an Employee’s laptop, cell phone or briefcase containing Personal Information is stolen; (ii) an Employee accesses another Employee’s or customer’s Personal Information for an unauthorized purpose (e.g., personal curiosity); or (iii) Otéra’s computer systems that host customer Personal Information are hacked or accessed by cybercriminals.

**“Information Asset”** means any resource providing elements of Information that is used by Otéra. This includes Information, documents, databases and business software packages, or a combination of these elements acquired or created within Otéra, whether or not they are hosted at Otéra or at the CDPQ.

**“Information Security Incident Response Plan”** means the plan drafted by the Chief, Ethics and Compliance in collaboration with the Vice-President and Chief Operating Officer and the Director, Enterprise Risk, that details, among other things, the Incident response process.

**“Laws respecting the protection of personal information”** or **“Applicable Laws”** means any laws, regulations, recommendations or notices applicable to matters relating to the protection of Personal Information, including, to the extent applicable, the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”), the *Act Respecting the Protection of Personal Information in the Private Sector* (the “Québec Private Sector Act”), European Union’s *General Data Protection Regulation* (“EU GDPR”), United Kingdom’s *General Data Protection Regulation* (“UK GDPR”) and the *Data Protection Act* 2018 (the “DPA”) (the DPA and the UK GDPR are collectively referred to as the “UK GDPR”) (the EU GDPR and the UK GDPR are collectively referred to as the “GDPR”), and any other laws, regulations, recommendations or notices that supersede, supplement, amend, extend, re-enact or codify the Laws respecting the protection of personal information.

**“Otéra”** means all entities doing business under the “Otéra” or “Otéra Capital” banner.

**“Personal Information”** means information relating to a natural person that allows that person to be identified, such as their name, identification number, geolocation data, online username, or to one or more factors specific to that person’s physical, physiological, genetic, mental, economic, cultural or social identity.

**“Processing”** means any operation or set of operations carried out with or without the use of automated processes and applied to data or sets of Personal Information (collection, use, recording, storage, modification, consultation, communication, dissemination, reconciliation, erasure, destruction, etc.).

**“Technology Asset”** means all hardware, software and services used for the collection, processing, and transmission of Information Assets. This includes, but is not limited to, workstations, telephones, tablets, keyboards and other data input or output devices. Software includes, but is not limited to, word processing software, desktop operating systems, servers and hardware, business software packages, network management tools, development tools, courseware and device drivers.

**“Transfer”** means any communication of Personal Information outside Québec, to another province or country.