Otéra
CDPQ

Guidelines on the Protection of Personal Information

Legal Affairs and Corporate Secretariat
March 31, 2023

Guidelines on the Protection of Personal Information

Team	Objective
Legal Affairs and Corporate Secretariat	**Description of how Otéra collects, uses, communicates and protects Personal Information and of how it can be accessed and corrected.**

Action	Approval authority	Date
Entry into force	Executive Committee	2022-11-15

Table of Contents

1. Definitions

In these guidelines, terms that are not defined in the main text are defined in Appendix 1.

2. Objective

Otéra places great importance on all Laws respecting the protection of personal information and is committed to maintaining the confidentiality of Personal Information. These guidelines briefly describe how Otéra collects, uses, communicates and protects Personal Information, and how it can be accessed and corrected when necessary.

3. Scope

These guidelines apply to Personal Information about identifiable individuals (collectively, the “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;
- members of the general public who contact Otéra to learn about its service offer;
- borrowers, partners and suppliers when Personal Information is collected in the course of their professional interactions with Otéra and its Employees;
- candidates for a position offered by Otéra;
- visitors to Otéra’s offices and website.

4. Processing of Personal Information

4.1. Collection of Personal Information

In the course of its activities, Otéra collects Personal Information limited to that which is necessary for the purposes of its collection.

4.2. Use of Personal Information

Personal Information may only be used for the legitimate legal or business purposes identified by Otéra at or before the time of collection.

4.3. Communication of Personal Information

Within Otéra – Personal Information processed within Otéra is accessible or communicated only to Otéra employees who need it to perform their duties, in accordance with the legal or legitimate business purposes identified by Otéra before or at the time of collection.

To third parties – 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.

For any Processing involving subcontractors or service providers (i.e., situations where Otéra retains the services of another organization that will process Personal Information on Otéra's behalf), Otéra puts in place agreements specifying the Processing instructions that the subcontractor or provider must follow. These relate particularly to the respect of people's rights, data security, notification of any Confidentiality Incident involving Personal Information, cross-border transfers, auditing and liability of the subcontractor.

Transfer of Personal Information outside Québec – Otéra may need to transfer or authorize access to Personal Information to parties based outside of Canada or the United States. A Transfer to another country, of Personal Information that is or will be subject to Processing after being transferred, can only take place if such information receives an equivalent or sufficient level of protection, in accordance with the Law.

Where required by Applicable Laws, Otéra shall conduct a Privacy Impact Assessment ("PIA") to ensure that such transferred Personal Information is adequately protected. The Privacy Officer is responsible for establishing procedures and practices to comply with this section and shall be consulted prior to any transfer to ensure that the PIA is conducted in accordance with the Applicable Law.

4.4. Retention of Personal Information

Otéra strives to keep Personal Information only as long as necessary to fulfill the purposes for which it was collected.

4.5. Security of Personal Information and Confidentiality Incidents

Otéra places great importance on data security. It strives to maintain physical, technical and administrative safeguards that are appropriate given the sensitivity of the Personal Information it seeks to protect. Consequently, Otéra and its subcontractors implement measures to ensure the confidentiality, integrity and protection of the Personal Information collected:

- **Physical measures** - These may include physical security measures, such as controls on access to premises, server rooms, wiring rooms, alarm systems, etc.
- **Technological measures** - To protect the data used by its Information Assets and Technological Assets, Otéra implements several security measures provided for in its policy on the security of information and technological assets.

- **Administrative measures** - To protect the data used by its various Information Assets and Technology Assets, Otéra implements several organizational measures, such as policies, guidelines, directives, and procedures.

4.6. Incident Management

Employees shall remain vigilant regarding Confidentiality Incidents and shall immediately report any actual or reasonably suspected Incident to the Incident Management Committee. This will allow Otéra to promptly investigate and respond to the Incident in accordance with its Information Security Incident Response Plan and related policies and procedures, and to protect Otéra, Data Subjects, and any other organization from any damage that may result therefrom.

Any request received under the applicable Laws shall be immediately forwarded to Otéra's Privacy Officer, at the following address: renseignementpersonnel@oteracapital.com.

5. Rights of the Data Subject

5.1. Access Rights

Otéra acknowledges that, in accordance with Applicable Laws, a data subject has the right to obtain confirmation as to the Processing of his or her Personal Information held by Otéra and to have access to it (i.e., to examine it and obtain a copy) without delay. In addition, computerized Personal Information collected from the Data Subject, and not created or inferred from Personal Information about the Data Subject, shall be provided to the Data Subject, at his or her request, in a structured and commonly used technological format.

5.2. Right to Rectification

Otéra acknowledges that, in accordance with Applicable Laws, a Data Subject has the right to have any Personal Information held by Otéra that is inaccurate or misleading corrected without delay and, in any event, within one month of Otéra's receipt of the request to correct inaccurate or misleading Personal Information.

Otéra further acknowledges that, given the purpose of the Processing, a Data Subject has the right to have his or her incomplete Personal Information completed, including by providing a supplementary statement.

Otéra also recognizes that, in accordance with the Québec Private Sector Act, an individual has the right to obtain the correction of Personal Information held by Otéra if its collection, communication or retention is not authorized by this Act.

5.3. Right to Withdraw Consent

In accordance with Applicable Laws, a Data Subject has the right to withdraw his or her consent to the Processing of his or her Personal Information at any time when the Processing of Personal Information is based on consent.

Otéra shall honour a Data Subject's request to withdraw consent, unless it is demonstrated that there are compelling legitimate grounds for the Processing that prevail over the interests and rights and freedoms of the Data Subject, or that the Processing is necessary for the establishment, exercise or defence of Otéra's legal claims.

6. Application Procedure

To exercise his or her rights, the Data Subject must submit a written request to the Privacy Officer. The Data Subject is encouraged to complete the request form according to the template developed by Otéra, without this form being mandatory. Otéra shall respond as soon as possible, but within a maximum of one month from the receipt of all relevant information. Otéra employees who receive a request from a Data Subject regarding his or her Personal Information shall notify the Privacy Officer and refrain from responding without the written authorization of the Privacy Officer. Otéra will retain documentation associated with requests (and related decisions) in accordance with the Retention Schedule.

7. Roles and Responsibilities

Executive Committee

- Review and approve these guidelines.
- Receive accountability from the Privacy Officer.
- Be notified of any significant Privacy Incidents.

Privacy Officer

- Ensure the implementation of Otéra's responsibilities under the Privacy Laws, particularly with respect to the protection of Personal Information.
- Update the *Policy Respecting the Protection of Personal Information* or these guidelines or other related procedures, as required.
- Ensure compliance with the implementation of the Laws respecting the protection of personal information.
- Identify, evaluate, remedy and monitor any issue relating to the protection of Personal Information by Otéra.
- Ensure that policies, procedures and other relevant practices are developed, implemented and maintained in accordance with these guidelines and the Laws respecting the protection of personal information.

- Develop and adopt notices, forms or terms of use for Otéra's websites in compliance with these guidelines and the Laws respecting the protection of personal information.

- Ensure awareness and training of employees regarding their duties, roles and responsibilities when dealing with Personal Information.

- Advise Otéra on any practical application of the Laws respecting the protection of personal information

- Ensure requests and complaints from Data Subjects in relation to their Personal Information are handled in accordance with these guidelines and Applicable Laws.

- Collaborate with Otéra's teams to ensure the security and protection of the confidentiality of Personal Information by Otéra.

- When required under Applicable Laws, collaborate with the Legal Affairs and Corporate Secretariat Group in conducting any Privacy Impact Assessment.

- In the context of a Confidentiality Incident, record any Incident in the Confidentiality Incident Register, assess the risk of serious injury, and notify the appropriate authorities and the Data Subjects when required.

- Report annually to the Executive Committee and the Governance and Ethics Committee on the implementation of the management framework for the *Policy Respecting the Protection of Personal Information.*

- Promptly notify the Executive Committee and the Governance and Ethics Committee of any material Confidentiality Incident.

Appendix 1: Definitions

For the purposes of these guidelines:

“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 the Data Subjects.

“Employees” means collectively the interns, 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.

“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.

“Privacy Officer” means the Privacy Officer designated (from time to time) by Otéra. As of the date hereof, the Privacy Officer is Otéra’s Chief Ethics and Compliance Officer.

“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.).

“Retention Schedule” means the schedule that establishes, among other things, the lifespan of a record from the time it is created until the time it must be destroyed or permanently retained.

“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.