Otéra
Caisse de dépôt et placement du Québec

Policy respecting the protection of personal information

GROUP / Team	OBJECTIVE
Human Resources and Corporate Services	The purpose of the Policy is to set out the Corporation's undertakings regarding the protection of personal information and to explicitly recognize the right of each individual to the confidentiality of their personal information, as well as to examine and establish, where applicable, the principles and methods for collecting, using, disclosing and safeguarding personal information.

TABLE OF CONTENTS

1. Introduction 3
2. Accountability 3
3. Scope 3
4. Effective Date 3
5. Principles of confidentiality 3
6. Purposes for which personal information is collected 5
7. Obtaining consent 5
8. Definitions 5
9. Third party providers 6
10. Technology watch and personal information 7
11. Checklist to insure compliance with the policy respecting the protection of personal information 7
12. Contact details 8

Schedule A 9

Schedule B 10

1. Introduction

The services provided by Otéra Capital inc. (hereinafter the “Corporation”) rely in part on the collection, use and disclosure of personal information concerning clients, partners and employees. The protection of personal information concerning them is one of the Corporation’s priorities. Therefore, the Corporation wishes to adopt a policy respecting the protection of personal information (hereinafter the “Policy”).

The purpose of the Policy is to set out the Corporation’s undertakings regarding the protection of personal information and to explicitly recognize the right of each individual to the confidentiality of their personal information, as well as to examine and establish, where applicable, the principles and methods for collecting, using, disclosing and safeguarding personal information.

2. Accountability

It shall ultimately be the responsibility of the Corporation’s Executive Committee to ensure compliance with this Policy.

3. Scope

The Corporation shall follow a policy respecting the protection of personal information it collects, uses and discloses concerning its employees, clients and partners. For such purposes, employees shall include the Corporation’s past and present employees and independent contractors.

The Corporation’s Policy shall apply to the collection, use, disclosure and retention of personal information in any form, be it verbal, electronic or written.

4. Effective Date

This Policy shall take effect on March 13, 2014.

5. Principles of confidentiality

The Corporation shall follow and comply with each of the following ten fair principles regarding information:

Principle 1 - Accountability

The Corporation shall be responsible for the personal information in its custody and has appointed privacy protection officers charged with ensuring it abides by these principles.

Principle 2 - Stating the purposes for which personal information is collected

The Corporation shall state the purposes for which it is collecting personal information at or before the time it collects the information.

Principle 3 - Obtaining consent to the collection, use or disclosure of personal information

The Corporation shall inform the individual whose personal information it is collecting, using or disclosing that it will be doing so and obtain the individual's consent to do so.

Principle 4 - Limiting the collection of personal information

The Corporation shall limit the collection of personal information to the minimum necessary for its stated legitimate purposes. The Corporation shall use fair and lawful means to collect personal information.

Principle 5 - Limiting use, disclosure and retention

The Corporation shall not use or disclose personal information for purposes other than those for which the information was collected, except if it has obtained the individual's consent or if required by law.

The Corporation shall retain personal information only for as long as necessary to satisfy the purposes for which it was collected. Thereafter, the information in question shall be destroyed or deleted within a reasonable period and by appropriate means of destruction or deletion (shredder, confidential destruction bin, etc.).

Principle 6 - Accuracy of personal information

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it was obtained.

Principle 7 - Safeguards

The Corporation shall protect personal information using means appropriate to the form and sensitivity of the information. These safeguards may include locks on filing cabinets and doors, restricted access to offices, computer safeguards (including user names and passwords, firewalls and encryption) as well as security protocols to ensure that access to personal information is provided only where needed.

Principle 8 - Openness with respect to policies and practices

The Corporation shall make available information about its policies and practices relating to the management of personal information.

Principle 9 - Individual access

Upon request, the Corporation shall inform an individual whether or not it holds personal information about the individual and, if so, disclose the information to the individual. An individual shall be entitled to challenge the accuracy and completeness of the personal information and have it amended, where applicable.

Protocol for accessing personal information

See Schedule A.

Principle 10 - Challenging compliance

An individual shall be entitled to challenge compliance with the above principles by addressing the challenge to the privacy protection officer charged with ensuring that the Corporation observes the Policy.

Protocol for challenging compliance

See Schedule B.

6. Purposes for which personal information is collected

The Corporation has collected personal information and will continue to do so for the following purposes:

- establishing and maintaining responsible business dealings with clients and partners in order to offer uninterrupted service;
- understanding the needs of its clients and partners;
- developing, improving, marketing and supplying products and services;
- managing and expanding its operations;
- satisfying its statutory and regulatory obligations, including protecting and defending legal interests; and
- establishing, managing and terminating employment relationships.

7. Obtaining consent

The Corporation shall endeavour to ensure that individuals understand how it will use their personal information. It shall obtain their consent at or before the time it collects or uses personal information concerning them.

The Corporation shall not use falsehoods or deceptive means to obtain an individual's consent.

The Corporation shall be entitled to collect, use or disclose personal information without an individual's knowledge or consent in specific cases permitted or required by law.

8. Definitions

Personal information

"Personal information" shall include information, whether or not recorded, concerning an identifiable individual. Regardless of its format, this information shall include:

- age, name, gender, identification numbers and income;
- opinions, evaluations, comments, matrimonial status and disciplinary measures;

- employee records, credit, loan or medical records, the existence of a dispute between a client and a merchant, intent (to acquire goods or services, change jobs, etc.) and past employment or financial history; and

- in addition, given the meaning attributed by the Corporation to the term “employee”, “personal information” shall include home address and telephone number, social insurance number, passwords, licence plate numbers, interests and leisure activities.

Personal information shall not include an individual’s name, title, address or telephone number at work. The exception for work-related information is intended to allow for the pursuit of day-to-day business activities.

In accordance with the Corporation’s practices, an individual’s home address and telephone number fall within the category of confidential information and shall therefore be considered and treated as such.

Consent

“Consent” shall mean the voluntary agreement to allow the use of personal information within the scope of a current or proposed action. Consent may be express or implied. “Express consent” shall be given explicitly, by being spoken out loud or stated in writing. It shall be unequivocal and involve no insinuation. “Implied consent” shall mean consent that can reasonably be inferred from an individual’s action or inaction.

If the Corporation modifies its use of personal information, it shall obtain a new consent in that regard. There shall be no provision for the protection of acquired rights.

Disclosure

“Disclosure” shall mean the act of making personal information available to third parties external to the Corporation.

Use

“Use” shall mean the handling and management of personal information within the Corporation.

9. Third party providers

The Corporation mandates third party providers to provide it with services in various sectors.

The Corporation shall request that its third party providers use appropriate safeguards to protect the personal information against unauthorized access, use or disclosure and that such third party providers shall not use or disclose the personal information entrusted to them by the Corporation for other purposes. The Corporation shall ensure that its third party providers use specific standardized methods to protect personal information and that these principles prohibit the collection, use or disclosure of information other than for purposes of the express mandate given to the provider. Some third-party providers may be located outside Canada, and personal information may therefore be subject to the laws of those other jurisdictions, in particular the laws providing access to this information by the appropriate government authorities.

The Corporation may enter into joint ventures or other strategic alliances liable to lead to the exchange of personal information. In such a case, the Corporation shall obtain the necessary consent for the collection, use and disclosure of the personal information and comply therewith.

10. Technology watch and personal information

The Corporation's technological tools, comprised of all its computer tools, multimedia tools and communications tools, including access to the Internet, computers, servers and storage media, and the use thereof shall be secured in accordance with the Corporation's policies procedures and business practices in effect. Please refer to the general policy entitled "General policy governing the use of information systems".

Personal information saved with the technological tools mentioned hereinabove as well as personal information kept through the reasonable use of the Internet shall be stored in accordance with the Corporation's policies, procedures and business practices in effect.

The information systems department shall not wilfully investigate the misuse of a technological tool or personal information with respect to a particular individual without first consulting the privacy protection officer. Where the privacy protection officer is presented with evidence of misconduct or a breach of the Corporation's policies, procedures or business practices in effect (regarding information technology governing access to personal information and its use), the Corporation shall have the right to access and examine the usage history for said technological tools without the prior consent of the individual concerned.

11. Checklist to insure compliance with the policy respecting the protection of personal information

The Company shall routinely check the methods it has implemented for the management of personal information. The following checklist will help departments determine whether they are compliant.

- Does your department collect personal information about individuals?
- For what reasons?
    - Is the individual concerned informed before the collection of data (personal information) or at that time?
    - Is everything recorded in a document?
    - Was the consent given verbally? Was it recorded in a document?
- How is the data (personal information) collected and used (verbally, in writing or electronically)?
- How is the data (personal information) protected? For example, who has access to it and where is it stored (physical or technological protection measures or protection protocol)?
- What are the retention periods before deletion, and what methods are used in this regard?
- How is the data (personal information) transmitted between the various departments, providers, partners or third parties external to the Corporation (by fax, e-mail or courier)? Is there an agreement in place to oversee this transfer and this use of data?

- If personal information is being sent to foreign third-party providers:
    - Are the people concerned notified of this?
    - Do you keep a list of these third-party providers, with their geographic locations and the purposes for which the personal information is being sent to them?

12. Contact details

Questions or concerns about the Corporation's Policy, protocols or methods for managing personal information and confidentiality, including its policies regarding foreign third-party providers, may be addressed:

- in writing, to Lysiane Roy, Vice-President, Human Resources and Corporate Services, privacy protection officer, Human Resources and Corporate Services Department
- by e-mail, to the following address: lroy@oteracapital.com
- by phone, at 514-847-5402

or

- in writing, to Jamila Ladjimi, Executive Vice-President and Chief Operating Officer, privacy protection officer
- by e-mail, to the following address: jladjimi@oteracapital.com
- by phone, at 514-847-5479

Concerns of a legal nature involving the Policy may be addressed:

- in writing, to Mélanie Charbonneau, Vice-President, Legal Affairs and Corporate Secretary
- by e-mail, to the following address: mcharbonneau@oteracapital.com
- by phone, at 514-847-5407

This Policy may be amended pursuant to legislative amendments. The Corporation reserves the right to amend this Policy at any time. Examples set out in this document are not exhaustive.

Schedule A

PROTOCOL - Accessing Personal Information

1. An individual wishing to access personal information shall make a written application to the privacy protection officer.

   The application shall contain the following elements:

   - the date on which the application is being made;
   - the department from which the individual wishes to obtain the information;
   - the period of time during which the individual wishes to access the personal information; and
   - the precise nature of the personal information requested.

2. The privacy protection officer shall provide the applicant with an acknowledgement of receipt of the application. In order to quickly process the application, the privacy protection officer may request clarifications or additional information.

3. The privacy protection officer shall examine the application and follow up thereon within 30 days of its receipt. The applicant shall be informed in writing whether the application has been refused or accepted. If access is refused, the reasons therefor and the applicant's recourses shall be stated.

4. Where an ordinary application for access is accepted, the personal information requested shall be provided to the applicant. Access to the personal information may be subject to the payment of a reasonable charge for the transcription, reproduction or transmission of the personal information.

Schedule B

PROTOCOL - Challenging Compliance

1. An individual wishing to file a complaint alleging non-compliance with the policy respecting the collection, use or disclosure of personal information shall do so in writing to the privacy protection officer.

   The complaint shall contain the following elements:

   - the date the complaint is being filed;
   - the department against which the complaint is being filed;
   - the date on which the incident occurred; and
   - the specific reason for the complaint.

2. The privacy protection officer shall provide the complainant with an acknowledgement of receipt of the complaint. In order to quickly process the complaint, the privacy protection officer may request clarifications or additional information.

3. The privacy protection officer shall examine the complaint and follow up thereon within 30 days of its receipt. The complainant shall be informed in writing of the decision rendered.

4. The privacy protection officer shall ensure that the necessary measures are taken to correct inaccurate personal information or modify policies and practices based on the outcome of a complaint and shall ensure that these modifications are communicated to the Corporation's employees via the intranet.

ANNUAL STATEMENT OF COMPLIANCE WITH OTERA CAPITAL INC.'S POLICY RESPECTING THE PROTECTION OF PERSONAL INFORMATION

I, the undersigned, _____ , hereby acknowledge that I have read and understood the meaning and scope of Otéra Capital inc.'s Policy respecting the protection of personal information. I agree to comply with the requirements of the Policy.

Signature: _____

Title: _____

Group: _____

Date: _____

Immediate supervisor: _____

(as witness) (Signature)

Immediate supervisor: _____

(as witness) (Name in block letters)

Date : _____

Please return the last page of this document, duly signed, to the Human Resources Department.