

<b>Document and Version:</b>	General – Policy – Personal Information Protection Policy	<b>Published on:</b>	04-18-2018
<b>Approved by:</b>	CST	<b>Revised on:</b>	10-12-2023
<b>Signature:</b>		<b>Confidentiality Level:</b>	Public

### Table of Contents

1.	Fino's Personal Information Protection Policy .....	2
2.	Appendix.....	5
2.1.	Document Properties .....	5
2.2.	Version control.....	5

## 1. Fino's Personal Information Protection Policy

As a market research and customer contact firm, Fino Research and Client Relations (hereinafter referred to as Fino) regularly collects personal information from individuals it surveys or interacts with in the course of client relationship management mandates entrusted to it by its clients. These individuals are referred to as "Participants" in this policy.

Fino is committed to safeguarding the personal information it holds, as well as any other forms of personal information it possesses.

Fino adheres to the Personal Information Protection and Electronic Documents Act. This policy has been developed based on the principles outlined in this national standard. The requirements of this federal law can be reviewed online at the following address: <https://laws-lois.justice.gc.ca/fra/Lois/P-8.6/index.html>, or a copy of the law and information about it can be obtained at the following number: 613-957-4222.

Furthermore, Fino is in the process of obtaining **SOC 2 Type II** certification. SOC stands for System and Organization Controls and represents a set of compliance standards developed by the American Institute of CPAs (AICPA). SOC audits aim to review an organization's policies, procedures, and internal controls. SOC 2 describes the standards necessary to preserve the confidentiality and security of sensitive data when it is in transit or at rest. By obtaining this certification, Fino demonstrates that privacy, confidentiality, and data integrity for its clients and employees are a top priority.

Fino is responsible for the personal information it manages and has designated Alexandre Meunier, an associate at Fino, as the Personal Information Protection Officer. He is responsible for:

- Implementing procedures to protect personal information.
- Establishing procedures for receiving and addressing complaints and information requests.
- Providing training to staff and conveying information about the organization's policies and practices.
- Drafting explanatory documents regarding its policies and procedures.

For any questions or information requests regarding the use of your personal information at Fino, please contact Alexandre Meunier, the Personal Information Protection Officer.

Email: [renseignements-personnels@finoconseil.com](mailto:renseignements-personnels@finoconseil.com)

Address: 2370 Galt Street West, Suite 100, Sherbrooke, QC, J1K 2W7

In the projects it undertakes, Fino commits to:

- Determine the purposes for which personal information will be collected before the start of the collection. The collection needs are typically determined in client tenders and/or Fino's service offerings.
- Collect or use only the personal information identified as essential for the mandate's purposes. The collected personal information is used solely for the project for which it was gathered.

- Identify itself at the beginning of any customer service call, interview, or survey and inform the participant of the project's objective, the purposes for collecting personal information, and the confidentiality of the shared information.
- Ensure participant consent is obtained before commencing information collection. This consent is obtained verbally during interviews and implicitly when the participant completes an online form or survey.
- Respond to participant questions regarding data usage purposes.
- Respond to participant questions regarding the source of their contact information.
- Respect the decision of a participant who does not wish to participate in a project or answer one or more questions.
- When Fino receives lists of clients or potential clients from its clients for a mandate, it is the client's responsibility to have obtained prior consent for the transmission of information to a third party.
- Not disclose personal information collected in the form of surveys, focus groups, interviews, or other customer contact projects to a third party (other than the client under certain provisions mentioned in this policy). The only circumstances in which personal information can be provided to a third party are when the respondent has been informed, and consent has been obtained, or when the law obligates us to provide such information (e.g., a subpoena or other legal requirement).
- Specifically, for all research projects:
  - Depersonalize working documents to limit the number containing personal information.
  - Aggregate respondent responses with those of other respondents so that it is never possible to identify a specific individual when reviewing the data.
  - Provide anonymized databases making participant identification impossible.
  - In rare cases, a nominal database may be provided to the client to allow them to add information from their internal databases and complete analyses (confidential information they do not wish to share with Fino). A prior agreement is signed at the beginning of the mandate, specifying the purposes of data usage and the responsibilities of Fino and the client.
- Specifically, for client relationship management projects (customer service, lead generation, appointment scheduling, nomination management, telemarketing, etc.):
  - The nature of these projects often involves the transmission of personal information and nominal data collected by Fino on behalf of its clients. This data is only shared with the client who has previously signed an agreement specifying the purposes of data usage and the responsibilities of Fino and the client.
  - During the mandate, Fino depersonalizes working documents to limit the number containing personal information.
- Destroy or anonymize all documents containing personal information when Fino's mandate is complete.
- Implement precise data collection tools and quality control processes to ensure the accuracy of collected personal information.

- Take all reasonable measures to ensure that data accessed on a regular basis is as up-to-date as possible when used.
- Train its team (project managers, analysts, supervisors, and agents) so that all employees adhere to the personal information protection policies and procedures put in place for data security. Each employee must sign a confidentiality agreement in which they commit to using personal information only for the mandates entrusted to them and understand that they could face disciplinary measures if they fail to comply.
- Protect personal information using security measures such as password protection on electronic files, two-factor authentication, encryption, sensitive data isolation, shredding of confidential documents by a specialized document security company, and access restrictions on physical premises with access to confidential data.
- Make its Personal Information Protection Policy available to the public.
- Inform any individual requesting it of the existence of personal information concerning them, its usage, and whether it has been shared with third parties (if applicable), and allow them to review it. Participants have the option to challenge the accuracy and completeness of information about them and request appropriate corrections. Requests for viewing and modifications should be addressed to Alexandre Meunier, the Personal Information Protection Officer.
  - Email: [renseignements-personnels@finoconseil.com](mailto:renseignements-personnels@finoconseil.com)
  - Address: 2370 Galt Street West, Suite 100, Sherbrooke, QC, J1K 2W7

Complaints regarding Fino's non-compliance with this policy can be directed to Alexandre Meunier, the Personal Information Protection Officer (see contact information above).

## 2. Appendix

### 2.1. Document Properties

Attributes	Details
Title	General – Policy – Personal Information Protection Policy
Version	01
Author	Alexandre Meunier
Document Classification	Public

### 2.2. Version control

Version	Date	Author	Description
01	04-18-2018	Alexandre Meunier	First draft
01	05-30-2023	Sophie Hallée	Revision
01	10-12-2023	Sophie Hallée	Revision