

# SOM'S POLICIES AND PRACTICES WITH RESPECT TO THE PROTECTION OF PERSONAL INFORMATION

---

## INTRODUCTION

SOM inc. is a company that specializes in social and market research, as well as in public opinion polling. SOM collects and processes large quantities of data (opinions, perceptions, habits, social and demographic characteristics) provided by individuals or companies on a daily basis. Most of the time, those who gave us the information cannot be identified. However, this is not always the case. It is sometimes possible to identify (name, telephone number or address) the individual or the organization that has given us the information. In this case, all information provided is termed: Personal Information.

Throughout the years, SOM has implemented several procedures to insure the confidentiality of personal information. This document details these measures and is based on the Canadian Privacy Act. This Privacy Code is based on 10 interrelated principles:

- Accountability
- Identifying purposes for Personal Data Collection
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

---

<sup>1</sup>- Source : Canadian Standards Association

## 1. ACCOUNTABILITY

**PRINCIPLE:**

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

**MEASURE(S) TAKEN BY SOM:**

SOM appoints Mr. Gilles Therrien, President, to oversee the organization's compliance with the procedures implemented to protect personal information collected and processed by our company.

On behalf of SOM inc., Mr. Therrien is responsible for:

- Implementing policies and practices to protect personal information in SOM's possession.
- Establishing procedures to receive and to respond to complaints and inquiries.
- Training staff and communicating to staff information about the organization's policy and practices.
- Drafting documents to explain the organization's policies and procedures.

## 2. IDENTIFYING PURPOSES FOR PERSONAL DATA COLLECTION

**PRINCIPLE:**

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

**MEASURE(S) TAKEN BY SOM:**

Except for a few cases, personal information is collected by SOM on behalf of one of its clients.

In such cases, the purposes for which personal information is collected are known prior to the start of the collection and are documented by SOM's client, either in a request for proposal, a research brief or in a written confirmation of a verbal agreement with the project manager.

Also, at the time of collection, right after the interviewer introduces himself, the purpose for which information is collected is mentioned, even before the respondent's consent is obtained.

In fact, all interviewers at SOM go through a specific training period before the start of every data collection. During this training session, explanations are given to them concerning the purpose for which information is collected, so that they will be able to explain it clearly to the respondent and in order to obtain his/her consent.

When conducting omnibus surveys, SOM collects and retains personal information (first name, telephone number and e-mail address) of those who agree to take part in Internet surveys and qualitative studies (focus groups). The interviewer tells the respondent orally, at the time the questionnaire is administered, the purpose for which the information is being gathered, that is prior to obtaining his/her consent.

### 3. CONSENT

**PRINCIPLE:**

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

**MEASURE(S) TAKEN BY SOM:**

Whether the method used to carry out the survey is the telephone, mail, in person, focus groups or in-depth interviews, the respondents' participation to SOM's surveys is always on a voluntary basis and SOM's interviewers never oblige any respondents or individuals to complete a questionnaire or even to answer a particular question. Also, at any given time, the respondent is able to end the interview, without further implications by SOM for such withdrawal.

For interviews carried out over the phone, in person, during focus groups and in-depth interviews, the interviewer or the recruiting agent seeks the respondent's consent after he/she has been introduced and has explained the purpose of the survey.

For surveys carried out by mail or using the Internet, the fact that the respondent agrees to answer the questions is an implied consent.

However, in a case where one of SOM's clients supplies a list of his/her current and potential clients to be used for a survey, focus group or an in-depth interview, SOM will never be responsible for seeking consent from these individuals or companies from whom this information was acquired.

This responsibility will be that of SOM's client.

Except in very exceptional circumstances, SOM never transmits personal information to a third party (other than to the client).

Even databases containing personal information are anonymized (purged of information that could identify an individual) before they are returned to our clients, unless a specific request is received to the effect that our client wishes to transfer and to add data to it from his/her own in-house databases. In most cases, such a request occurs when the information is considered very confidential and the client does not wish to communicate it to us in the sampling database in order to protect it.

For focus groups, SOM takes necessary measures to ensure that participants are not totally identified on recruitment grids or during conversations. Only the participant's first name is used when addressing the person or when writing his/her name down on recruitment grids. Consequently, seeking consent is not required in this situation.

SOM does not use the PMRS central file listing all participants to focus groups. Therefore, SOM does not supply this organization with any personal information. The participant's consent is not required in this case either.

When conducting focus groups, there is only one incident where a participant's full name is given to a third party. This happens when the list of participants is given to a sub-contractor supplying room rental for the meetings. This list is used to collect the participants' signature as confirmation for having received a monetary compensation for their attendance. In this precise situation, SOM seeks the participant's consent to the effect that his/her name be given to the room rental agency for identification purposes when payment is made.

#### 4. LIMITING COLLECTION

**PRINCIPLE:**

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

**MEASURE(S) TAKEN BY SOM:**

For all sales contracts carried out for its clients, where personal information is either supplied or collected, SOM undertakes not to collect any information for its own use or for any purpose other than that required and pre-determined by or with its client.

In other terms, SOM will not use surveys, focus groups or personal interviews carried out on behalf of its clients for the purpose of obtaining personal information from respondents and from which it could profit.

## 5. LIMITING USE, DISCLOSURE, AND RETENTION

### **PRINCIPLE:**

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

### **MEASURE(S) TAKEN BY SOM:**

For all of its contracts, SOM undertakes not to use the information collected for any purpose other than that required by its clients.

Every interviewer employed by SOM is required to sign a Confidentiality Agreement stating that he/she will not use personal information for any purpose other than that stipulated in the sales contract and that he/she runs the risk of persecution (suspension, dismissal, legal action) for failing to respect the terms of this agreement (See Appendix A).

Data files and hard copies containing personal information are kept until we receive written authorization from our client to proceed with their disposal.

Paper copies are disposed of by shredding and data files on SOM's computer systems are deleted using a Secure Delete program.

## 6. ACCURACY

### PRINCIPLE:

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

### MEASURE(S) TAKEN BY SOM:

#### **Information supplied by our clients**

Our clients are responsible for the accuracy of personal information contained on the lists they provide us with for sampling and recruitment purposes.

However, SOM verifies all lists supplied for sampling and recruitment purposes to make sure they contain all the information required for sampling selection. When the lists fail to meet this requirement, they are returned to the client for correction.

#### **Competent and reliable interviewing staff**

To guarantee accuracy of personal information collected, SOM begins by recruiting competent staff and providing close training and supervision, as well as designing precise questionnaires, focus group or interview guides.

SOM has very specific requirements when it comes to recruiting skilled interviewers. Those we employ must:

- Express themselves clearly and with confidence
- Clearly demonstrate their ability to understand and to integrate established standards in order to carry out interviews of good quality
- Be honest
- Be bilingual

As soon as they join our ranks, all interviewers receive six and a half hours of general training on how to approach and interview people while remaining as unbiased as possible. This initial training is complemented by on-going training given directly by the supervisor.

Also, for every project, the designated manager briefs the interviewers on the particularities of the questionnaire. Every question is read and explained if required, as well as every response option and its meaning.

### **Clear questionnaires and guides**

Questionnaires and focus group or interview guides are designed by analysts or project managers then revised by a methodological expert to make sure the questions and their response options are clear, that they are asked in a logical order and that no bias is introduced or wrong skip patterns used.

The questionnaires are pre-tested with a certain number of respondents to make sure, among other reasons, that the questions and the response options are well understood and skip patterns are correctly programmed.

Questionnaire must bear client's approval before and after pre-testing is carried out.

### **Error-proof Data Entry System**

Our telephone surveys are carried out using a Computer Assisted Telephone Interview system (CATI). Our system imports the questionnaires directly in Word format to eliminate retranscription errors.

It also automatically validates answers given by the respondent and entered by the interviewer, thus avoiding any mistakes.

Our CATI system (Computer Assisted Telephone Interview) is adapted for Internet surveys. The same data validation options are available to eliminate any wrong entries.

When recording answers for surveys carried out in person or by mail, the information is entered twice (double entry), also in order to eliminate any errors.

## 7. SAFEGUARDS

### PRINCIPLE:

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

### MEASURE(S) TAKEN BY SOM:

#### **Receipt of personal information**

From the time clients send us personal information to be used for sampling and recruitment purposes, and up until we receive it, our clients remain responsible for the safeguards of personal information.

When personal information is received, it is transferred to a survey technician assigned to confidential projects and any copy of the file is deleted or destroyed following this internal transfer.

The survey technician clearly marks the file containing personal information (using the letters NBK or NOBKP in the file's title) so that no permanent backup copy may be produced automatically by our system.

Pending their use, at the end of every working day, as well as after using them, hard copy lists are kept in a locked filing cabinet.

All employees required to handle personal information must sign a Commitment to protect personal information before the start of a specific project (See Appendix B)

#### **Computerized safeguards for the storage of data**

Personal information stored on the computer system (either provided by our client or collected by SOM), is protected by several computer security measures.

These computer security measures of protection are updated periodically to reflect changes with respect to new environment, changes in safeguard requirements, improvement against new virus attacks or against any other attacks that would render our computer system vulnerable.

SOM's computer security measures:

- Provide constant access to all computer programs and equipment.
- Guarantee total integrity of all personal information stored on its computer system.
- Preserve confidentiality of this personal information.

To reach the required level of protection, SOM has set the following goal: to protect the company's computer systems against all risks in a manner that is appropriate for the company, its working environment and the condition of its computer equipment.

### **Identification and risks analysis**

To incorporate these computer security measures properly, SOM identifies the risks and hazards, whether or not their origin is internal or external or else whether they occurred accidentally or intentionally; this method involves identifying which computer systems are vulnerable and thus pose serious threats.

Also, for every one of them, SOM establishes a critical threshold in order to establish a good equilibrium between risks versus protection costs.

### **The measures taken to...**

...guarantee continuous access to all of SOM's computers:

- Assign a computer technician responsible for the maintenance of all computer systems.
- Redondant disks equipped with RAID systems.
- Provide file servers with a UPS protection against short power outages.

...guarantee the integrity and the confidentiality of personal information stored by SOM on its computer system:

- a) Implementation of a method to eliminate the backup of files containing personal information and to store it in one location only.

b) Implementation of security measures for the network:

- Both of SOM offices have independent access to the Internet.
- All traffic between the local network and the Internet inevitably passes through a PIX firewall made by Cisco, limiting in-coming access to the bare necessity, that is access to Internet servers and to e-mail messages. Thus, it is impossible to have in-coming access to file servers, to personal computers owned by SOM's personnel and the Montreal office. The firewalls provide out-going access to the Internet from authorized computers only.
- Networking between both offices (Quebec City and Montreal) goes through a VPN encryption (on-line private network) kept in place permanently between the PIX of both offices.
- Abnormal PIX network activity is monitored.

c) Implementation of server security safeguards:

- Databases and files servers containing the data used by our production programs and applications are not accessible from outside of SOM's offices.
- Access to those servers requires a user's account and password that are given only to authorized technician on a "need-to-know" basis.
- The room where the servers are located is locked when the technician is absent from his desk.

d) Destruction and deletion of personal information at the end of a project:

- Upon receipt of a written authorization from our client, we destroy or delete personal information (lists supplied, data collected) at the end of the project. Files may be destroyed or deleted entirely or only information that would reveal a respondent's identity (for example: name, telephone number and/or address). This is done using a Secure Delete computer program that is specifically designed to override or delete information.

## 8. OPENNESS

**PRINCIPLE:**

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

**MEASURE(S) TAKEN BY SOM:**

A copy of SOM's policy with respect to the protection of personal information can be acquired following a written request addressed to the person in charge: Mr. Gilles Therrien.

It can also be obtained on SOM's website at [www.som.ca](http://www.som.ca) .

## 9. INDIVIDUAL ACCESS

### **PRINCIPLE:**

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

### **MEASURE(S) TAKEN BY SOM :**

When asked by a respondent how his/her name and telephone number was obtained, the interviewer is obliged to tell the truth and reveal how this information was acquired.

A respondent wishing to find out or to verify what information we hold on him/her may request the Project Manager to supply the answer within one week at the most.

Should a respondent wish to amend this information, he/she will be referred to the client who has supplied us with it initially.

Should a respondent wish to verify and to make changes to answers already given in a survey or during a focus group, his/her request should be addressed to the Project Manager. The Project Manager will comply with this request providing the information identifying the respondent was not destroyed or deleted following the client's written authorization to dispose of it.

## 10. CHALLENGING COMPLIANCE

**PRINCIPLE:**

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

**MEASURE(S) TAKEN BY SOM :**

Anyone wishing to address a challenge concerning the non-compliance with the principles stated in this policy may do so in writing or by phone with Mr. Gilles Therrien who is the individual in charge of this policy.

All complaints will be thoroughly investigated by SOM and appropriate measures and corrective actions will be taken if required.

A record will be kept for a minimum five year period of all written complaints as well as those received by e-mail. SOM's management will check this record periodically to see if its policy concerning the protection of personal information needs to be improved.

**APPENDIX « A »**

**CONFIDENTIALITY AGREEMENT**

I, the undersigned \_\_\_\_\_ formally declare that I was made

**(Name in print characters)**

aware of the confidential nature of the work and agree to keep all information, documents, software and computer programs belonging to SOM inc., as well as any other information collected in reference to the service offer, totally confidential during the entire duration and after completion of the agreement. This confidentiality agreement is unconditional and does not bear on the service agreement.

More specifically, I agree to:

- keep all work carried out for SOM inc., in complete confidentiality;
- never to disclose, either during or after termination of my employment with SOM, any information referring directly or indirectly to any of the surveys carried out or the name of the client by whom it was commissioned;
- respect the exclusivity of SOM's intellectual property with respect to all material or equipment used and not to, or to no longer use, in any way, any documents, models, software and computer programs obtained during my employment.

I acknowledge that by failing to respect any of the terms of this agreement, I will run the risk of persecution (dismissal) and legal action.

I acknowledge that by failing to respect the professional standards established by SOM could result in the termination of my employment.

The above Confidentiality Agreement is signed by \_\_\_\_\_

This \_\_\_\_\_ day of \_\_\_\_\_

## **APPENDIX « B »**

### **COMMITMENT TO PROTECT PERSONAL INFORMATION**

---

Based on the contract between SOM inc. and \_\_\_\_\_,  
(Client's name)

I acknowledge having to preserve the confidentiality of the personal information that I will have access to during my employment.

Therefore, I agree to fulfill the following obligations:

- not to use this information for purposes other than that required by the project;
- not to look for confidential information, not to read confidential documents or computer files for purposes other than that required to carry out my work and not to transmit or allow the transmission of information appearing in the files I have access to, unless this communication or disclosure is legal;
- not to look up information other than that relating to projects assigned to me and to disclose the facts or information obtained during my employment strictly if it is legally authorized;
- after project completion, to return all documents in my possession and containing personal information, irrespective of their format (written documents or computer data).

I have signed \_\_\_\_\_

In : \_\_\_\_\_, On \_\_\_\_\_