

PROCEDURE IN CASE OF A VIOLATION OF PRIVACY



Last updated August 1, 2018

TABLE OF CONTENTS

1. GENERAL PROVISIONS	3
2. OBJECTIVES	3
3. DEFINITIONS	3
A) Violation of privacy (breach of personal information)	3
B) Affected person	4
C) Interested person	4
D) Personal information	4
E) Sensitive personal information	4
F) Exporior Financial Group	4
4. STEPS TO FOLLOW	5
4.1 Limiting the breach and preliminary assessment	5
4.2 Assessment of risk associated with the violation	5
4.2.1 The personal information in question	6
4.2.2 Cause and extent of the breach	6
4.2.3 Affected persons	7
4.2.4 Foreseeable prejudice arising from the breach	7
4.3 Notification of the breach	8
4.3.1 Notice to affected and interested persons	8
4.3.2 How and when to advise affected and interested persons	8
4.3.2.1 When	9
4.3.2.2 How	9
4.3.2.3 Form and content of the notice	9
4.3.2.4 Other persons to advise	9
4.4 Future prevention	10
5. RESPONSIBILITIES	11
5.1 Management	11
5.2 Person responsible for the protection of personal information	11
5.3 Management staff members	11
5.4 Employees	11
5.5 Team in charge of the investigation	12

1. GENERAL PROVISIONS AND OBJECTIVES

Through its policy on the protection of personal information, Experior Financial Group reaffirms its commitment to protect such information and to comply with the laws and regulations that govern their management.

In this context, we believe it necessary to adopt measures that are to be applied in the case of a violation (breach) regarding the protection of personal information.

Although we have implemented protection measures that we deem appropriate, we cannot claim to be absolutely protected from a breach regarding the protection of personal information.

The objectives of this procedure are:

- to define responsibilities.
- to establish steps to be followed in the case of a violation (breach) of the protection of personal information, and,

2. DEFINITIONS

A) Violation of privacy (breach of personal information)

A violation of privacy is any suspected or actual non-authorized access to personal information, through the non- authorized consultation, collection, use or communication of such. A violation of privacy can also occur when personal information held by Experior Financial Group is:

- o stolen, lost or communicated by error and/or because of a procedural error or operational failure.

The present procedure must be applied for any violation, regardless of its gravity.

B) Affected person

Any person who is concerned by the violation of privacy. In other words, the person who the personal information is about.

C) Interested Person

Any person who is indirectly concerned by the violation, be it Experior Financial Group, its clients, suppliers, agents, the public or any other organization.

D) Personal Information

Information concerning an individual that allows such an individual to be identified.

E) Sensitive Personal Information

Personal information regarding health status, government issued identification documents, bank accounts, credit card numbers or any other information of the same nature.

F) Experior Financial Group

Includes Experior Financial Group, its employees, management staff, agents and representatives.

3. Procedural Steps

There are four main steps to consider in the event of a suspected or real breach, of data protection.

Steps 4.1, 4.2 and 4.3 are carried out simultaneously or quickly, one after the next, while step 4.4 includes recommendations for long-term solutions and prevention strategies. Each breach must be taken seriously and an investigation must be launched promptly.

4.1 Preliminary Assessment and Limiting the breach and

As soon as an employee, a management staff member, an agent, or a representative of Expor Financial Group learns of a breach or suspected breach, he/she must:

- a) Take all necessary means to limit the breach immediately by:
 - ending the non-authorized practice;
 - retrieving the files;
 - shutting down the system from which the breach originated;
 - revoking or modifying the computer access codes;
 - correcting the deficiencies in the material and computer security systems.

- b) Advise the person responsible for the protection of personal information who will:
 - designate a qualified person to conduct the initial investigation;
 - conduct an investigation and/or determine if it is necessary to create a team made up of persons from the sector concerned by the breach, a member of senior management and the crisis coordinator designated pursuant to the Business continuity policy;
 - determine, alone or with the help of the team, which persons need to be advised of the incident, internally and potentially externally;
 - notify the Chief compliance officer;
 - notify the police if the breach arises from a theft or any other criminal activity;
 - thoroughly document the file and not destroy any evidence that could help determine the cause of the incident or to take necessary corrective measures.

4.2 Assessment of risk associated with the violation

To determine what other measures need to be implemented, it is necessary to assess the risk associated with the violation as concerns the personal information and take the following factors into account:

4.2.1 The personal information in question

The (INSERT POSITION TITLE) will have to take into account the nature of the information, how sensitive it is, and the foreseeable prejudice for the affected and interested persons when assessing the risk.

- What information elements are in question?
- In what measure is this information sensitive?

Ex. : a combination of personal information elements is generally more sensitive than a single item of personal information.

- What is the context for the personal information in question?
- Is the personal information suitably encoded, depersonalized or hard to access?
- How can the personal information be used?
- Can the information be used for fraud or other prejudicial means?

Ex. : theft or misappropriation of identity

A proper assessment of the type of personal information in question will help determine the measures to take, the persons to notify, including the appropriate privacy commissioner, as well as the manner in which to notify affected persons.

4.2.2 Cause and extent of the breach

It is important to determine the cause of the breach to the extent possible. The person responsible for the protection of personal information and/or the team in charge of the investigation will need to verify the following:

- Is there a risk that this non-authorized access to personal information will continue or that the information will be further compromised?
- Was the information stolen or lost? If it was stolen, can we determine if the information was the purpose of the theft?
- Was the personal information recovered?
- What measures were taken to mitigate prejudice and/or damages?
- Is this a systemic problem or an isolated incident?

4.2.3 Affected persons

At this step, it is important to determine the three following aspects as much as possible:

- Establish who is affected by the breach (employees, clients, suppliers, etc.);
- Establish and quantify the amount of personal information affected by the breach;
- Establish who is likely to have received this personal information.

4.2.4 Foreseeable prejudice arising from the breach

The **person responsible for the protection** of personal information and/or the team in charge of the investigation assessing the risk of prejudice must take into account the reasonable expectations of both affected and interested persons with due diligence and consider the following elements:

- Is there a link between the unauthorized recipients and the persons affected by the information?

Ex. : Was the information communicated to an unknown person or someone suspected to be involved in criminal activity, or was the information communicated to a person who is known and trustworthy?

- What could be the nature of the prejudice to the affected and interested persons?

Ex. : Risk to physical safety, identity theft, misappropriation of identity, financial loss, commercial loss, possible loss of employment.

- What prejudice could the breach cause for Experior Financial Group?

Ex. : loss of trust, loss of assets, financial risks, civil or criminal lawsuit (class action).

4.3 Notification of the breach

Notification of the breach can be tricky in that it is difficult to determine which situations need to be reported.

Thus, every incident need to be analyzed on a case-by-case basis in order to determine if the violation of privacy needs to be reported and, if applicable, to whom.

If the breach becomes a risk of prejudice to the affected and interested persons, they should be informed of such as quickly as possible so they can take necessary means to protect themselves.

4.3.1 Notice to affected and interested persons

In order to decide if the affected and interested persons need to be advised, the following factors must be taken into account:

- What are the lawful and contractual obligations?
- What are the risks of prejudice for the affected and interested persons?
- Is it reasonable to suspect possible identity theft, misappropriation of identity or fraud?
- Is there a risk of personal injury for the affected person (being followed, victim of harassment)?
- Is there a risk of humiliation or injury to reputation (medical file, discipline record, mental health record) for the affected person?
- Can the affected person avoid or mitigate potential damage?

4.3.2 How and when to advise affected and interested persons

At this stage, a comprehensive list of facts has to be drawn up and the risks have been evaluated in order to determine if it is necessary to advise affected and interested persons.

4.3.2.1 When

The affected and interested persons must be advised as quickly as possible. However, if the law enforcement officials have seized the matter, it is preferable to ask them if the notification should be delayed in order to avoid compromising their investigation.

4.3.2.2 How

It is preferable to advise the persons directly, by telephone, mail and email, or in person. Indirect notification (website, public notice in newspapers, etc.) is not recommended.

4.3.2.3 Form and content of the notice

The content and form of the notice will vary depending on the breach and the notification method chosen, and should contain the following elements, if applicable:

- a brief description of the breach and the moment when it happened;
- a description of the personal information in question;
- a brief description of the measures taken to control or reduce prejudice;
- the measures taken by Experior Financial Group to help the persons and the measures that they can take for themselves in order to avoid or reduce the risk of prejudice and to further protect themselves (ex.: arrangements for credit watch; information on how to change one's social insurance number, health insurance number, driver's license; fraud prevention tools);
- information sources to help people protect themselves against identity theft and misappropriation of identity;
- contact information for a Experior Financial Group employee who can answer questions or provide more information;
- reporting of the breach to the privacy commissioner;
- how to reach us to share their comments with us;
- give the contact information for the privacy commissioner.

4.3.2.4 Other persons to advise

The **person responsible** for the protection of personal information and/or the team in charge of the investigation will advise the appropriate privacy commissioner of all cases of violation, if necessary, so that he may respond to information enquiries from the public or to any potential complaint, or so he may give useful advice.

In order to evaluate the need to report a privacy violation, the following factors must be taken into account:

- any applicable law requiring the notification;
- the type of personal information in question, including:
 - the information that was communicated,
 - if it can be used to commit a theft and/or
 - a misappropriation of identity
 - and if there is a reasonable risk of prejudice arising from the leak of this information, including non-financial losses;
- the number of persons affected or concerned by the breach;
- whether the affected or interested persons have been advised or not;
- if we must reasonably deduce that the privacy commissioner's office will receive complaints or requests for information concerning the violation.

If necessary, it is also important to consider advising the following persons,:

- the police, in case of theft or criminal activity;
- insurance companies or other pursuant to contractual obligations;
- professional corporations or other regulatory agencies, if standards so require;
- financial institutions, including insurance companies to the extent that their help is required to communicate with the affected or interested persons;
- any other person.

4.4 Future prevention

Once immediate measures have been taken to lessen the risk associated with the breach, **the person responsible** for the protection of personal information and/or the team in charge of the investigation must investigate the causes of the incident and establish a prevention plan, if necessary, taking the following elements into account:

- a verification of physical and technical security;
- a review of policies and procedures and their update;
- a review of training practices for employees;
- a review of provider practices.

Finally, a self-verification of the plan must be carried out at the end of the process to determine if it

meets expectations or not. → **What does this mean??**

4. RESPONSIBILITIES

5.1 Management

Members of the executive committee adopt the present procedure and name the person responsible for the protection of personal information as responsible for the application and implementation of the procedure.

5.2 Person responsible for the protection of personal information

Coordinates all investigations regarding a breach and sets up an investigative team. Keeps management aware of activities on a regular basis and seeks their approval when necessary.

Ensures that the present procedure is delivered and communicated to all employees.

Produces an annual report of his activities and presents it to the executive committee.

5.3 Management staff members

Management staff members respect the present procedure and ensure it is communicated to their employees.

They take all necessary means to limit, without delay, any violation they are made aware of and immediately report it to the person responsible for the protection of personal information. At his/her request, the management staff is part of the team in charge of the investigation.

5.4 Employees

Employees respect and comply with the present procedure. They advise their superior immediately or, if they cannot, the person responsible for the protection of personal information, of any breach. They take necessary measures to limit it immediately. At the request of the person responsible for the protection of personal information, they are part of the team in charge of the investigation.

5.5 Team in charge of the investigation

The persons appointed by the person responsible for the protection of personal information to be part of the investigation team must participate in each of the steps described in detail in the present policy.